

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

SERGIO DE JESÚS ZAPATA ESPINOSA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA EIBTI
INGENIERÍA ELECTRÓNICA
MEDELLÍN
2021

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

SERGIO DE JESÚS ZAPATA ESPINOSA

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR POR EL
TÍTULO DE INGENIERO ELECTRÓNICO

TUTOR
HECTOR MANUEL HERRERA HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
INGENIERÍA ELECTRÓNICA
MEDELLÍN
2021

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

MEDELLIN 12 DE JULIO DE 2021

Dedico este trabajo escrito a todas las personas que de una u otra forma se comprometieron con este proyecto personal, que decidí iniciar unos años atrás esperanzado en superar mis conocimientos y avizorando un mejor futuro profesional. Gracias a la vida que me permitió llegar hasta este momento a pesar de las dificultades que existen hoy en día en nuestro país, pero el deseo interminable de alcanzar una meta proyectada con un final feliz, me llena de gran emoción, sin olvidar a cada uno de mis familiares que senos adelantaron en el viaje de la vida y que me apoyaron con su gran amor y paciencia.

AGRADECIMIENTOS

Agradeciendo a todos aquellos compañeros con quienes compartí a lo largo de la carrera muchos momentos de apoyo, igualmente a los tutores por su orientación y compromiso con cada uno de nosotros, a la UNAD por darme la oportunidad de superarme a nivel académico y el conocimiento adquirido haciéndome una mejor persona, acrecentado los valores de ética y moral que debe tener un gran profesional.

Agradeciendo a todos mis amigos que me regalaron el espacio para poder desarrollar las diferentes actividades mientras se discutían situaciones complejas a nivel social y que por eso desde mi conocimiento adquirido trataré de aportar al desarrollo de una mejor comunidad.

También para los compañeros y superiores en cada una de las empresas que labore a lo largo de la carrera por su comprensión en los momentos que dije no tener disponibilidad, sólo por dedicarme a las actividades académicas y poder logra desarrollas de una manera efectiva.

CONTENIDO

	Pág.
AGRADECIMIENTOS.....	5
CONTENIDO.....	6
LISTA DE TABLAS.....	7
LISTA DE GRAFICAS.....	9
LISTA DE ANEXOS.....	11
GLOSARIO.....	12
RESUMEN.....	13
INTRODUCCION.....	14
OBJETIVOS.....	15
ESCENERIO 1.....	16
ESCENARIO 2.....	41
CONCLUSIONES.....	64
BIBLIOGRAFÍA.....	65

LISTA DE TABLAS

	Pág.
Tabla 1. VLAN Escenario 1.....	16
Tabla 2. Asignación direcciones Escenario 1.....	17
Tabla 3. Configuración R1 Escenario 1.....	20
Tabla 4. Configuración básica S1 y S2 Escenario 1.....	24
Tabla 5. Configuración infraestructura S1 Escenario 1.....	26
Tabla 6. Configuración infraestructura S2 Escenario 1.....	29
Tabla 7. Configuración soporte host R1 Escenario 1.....	31
Tabla 8. Configuración servidores Escenario 1.....	33
Tabla 9. Realizando PING extremo a extremo Escenario 1.....	33
Tabla 10. Inicializando Router y Switch Escenario 2.....	42
Tabla 11. Configuración PC Internet Escenario 2.....	42
Tabla 12. Configuración básica R1 Escenario 2.....	42
Tabla 13. Configuración básica R2 Escenario 2.....	43
Tabla 14. Configuración básica R3 Escenario 2.....	44
Tabla 15. Configuración básica S1 Escenario 2.....	45
Tabla 16. Configuración básica S3 Escenario 2.....	46
Tabla 17. Realizando PING R1, R2 y PC Escenario 2.....	46
Tabla 18. Configuración VLAN en S1 Escenario 2.....	46
Tabla 19. Configuración VLAN en S3 Escenario 2.....	47

Tabla 20. Configuración Infraestructura en R1 Escenario 2.....	48
Tabla 21. Realizando PING S1 y S3Escenario 2.....	49
Tabla 22. Configuración OSPF en R1Escenario 2.....	49
Tabla 23. Configuración OSPF en R2Escenario 2.....	50
Tabla 24. Configuración OSPF en R3 Escenario 2.....	50
Tabla 25. Utilizando Comando Show OSPF Escenario 2.....	51
Tabla 26. Configuración R1 como servidor DHCP Escenario2.....	51
Tabla 27. Configuración en R3 las NATEscenario 2.....	52
Tabla 28. Configuración protocolos DHCP y NATEscenario 2.....	53
Tabla 29. Configuración NTPEscenario 2.....	54
Tabla 30. Configuración en R2 ACL y VTYEscenario 2.....	54
Tabla 31. Verificando Configuración ACL y NATEscenario 2.....	54

LISTA DE GRÁFICAS

	Pág.
Gráfica 1. Show interface brief Escenario 1.....	34
Gráfica 2. Show ip route Escenario 1.....	35
Gráfica 3. Show ipv6 interface brief Escenario 1.....	35
Gráfica 4. Show vlanbrief Escenario 1.....	36
Gráfica 5. Sh int f0/1 switchport Escenario 1.....	36
Gráfica 6. Sh int f0/2 switchport Escenario 1.....	37
Gráfica 7. Sh Ethernet summary Escenario 1.....	37
Gráfica 8. Sh Etherchannel port-channel Escenario 1.....	38
Gráfica 9. Sh vlanbrief Escenario 1.....	38
Gráfica 10. Ipconfig /all PC-A Escenario 1.....	39
Gráfica 11. Ipconfig /all PC-B Escenario 1.....	39
Gráfica 12. Haciendo PING a PC-A Escenario 1.....	40
Gráfica 13. Haciendo PING a PC-B Escenario 1.....	40
Gráfica 14. Sh Protocolo LACP Escenario 1.....	41
Gráfica 15. Sh IPV6 route R2 Escenario 2.....	55
Gráfica 16. Sh IPV6 route R1 Escenario 2.....	56
Gráfica 17. Sh IPV6 route R3 Escenario 2.....	57
Gráfica 18. Realizando PING en R1 y R2 Escenario 2.....	58

Gráfica 19. Realizando PING en S1 y S2Escenario 2.....	58
Gráfica 20. Realizando PING en S3 y S2Escenario 2.....	59
Gráfica 21. Show ip protocolos en R3.Escenario 2.....	59
Gráfica 22. Show ip route OSPF en R3Escenario 2.....	60
Gráfica 23. Show ip OSPF en R3Escenario 2.....	60
Gráfica 24. Show ip protocolos en R1Escenario 2.....	61
Gráfica 25. Show ip OSPF en R1Escenario 2.....	62
Gráfica 26. Show NTP en R1Escenario 2.....	62
Gráfica 27. telnet en R1Escenario 2.....	63
Gráfica 28. telnet en R2Escenario 2.....	63

LISTA DE ANEXOS

	Pág.
Anexo A. Repositorio Handle UNAD.....	66
Anexo B. Artículo IEEE.....	66
Anexo C. Link Video Sustentación.....	66

GLOSARIO

IOS: Significa sistema operativo de interconexión el cual fue desarrollado por CISCO system con el fin de poder programar los equipos como router y switches de su marca

OSPF: Este protocolo denominado abrir el camino más corto primero por sus siglas en inglés (Open Shortest Path First) el cual usa el algoritmo dijkstra enlace-estado (LSA - Link State Algorithm) para poder determinar por medios de diferentes cálculos la ruta más corta.

ROUTER: Dispositivo que se usa en telecomunicaciones para determinar la vía más rápida de transferencia de datos entre diferentes redes tanto internas como externas

SWITCH: Dispositivo que transfiere paquetes de datos entre redes internas.

VLAN: Abreviación de red virtual de área local que corresponde a redes no físicas si no lógicas.

TRUNKING: Es una forma de referirse a una troncal que es la que permite el acceso a muchos usuarios.

RESUMEN

Con el presente trabajo se pretende dar a conocer y aprender a utilizar herramientas de simulación y laboratorios de acceso remoto con el fin de simular las diferentes topologías de redes que permitan dar información referente a los diferentes comportamientos de las redes LAN y WAN, utilizando varios protocolos y métricas que están establecidas para ellas en su enrutamiento, administración y solución de los diferentes problemas que pueden surgir en la configuración de dispositivos como router y switches.

PALABRAS CLAVE: VLAN, DHCP, Etherchannel , port-security, router, switches, IPv4 y IPv6

1. INTRODUCCIÓN

Con el presente trabajo daremos solución a dos escenarios que se plantean, donde se pretende desarrollar las habilidades en cuanto a configuración de router, switches, PC con IPv4 y IPv6, igualmente configuración de enrutamiento entre VLAN, DHCP, Etherchannel y port-security. Aunque en los dos escenarios se incluyen en su mayoría equipos iguales y que en su configuración inicial no cambia ya que es la básica en ambos entornos corporativos se manejan configuraciones avanzadas diferentes lo que conlleva a profundizar en comandos diferentes y totalmente novedosos para los que incursionamos en el mundo de las redes de comunicación.

En el segundo Escenario se configuraran parámetros relacionados con el protocolo de routing dinámico OSPF, traducción de direccionamiento de redes dinámicas y estáticas NAT, protocolo de tiempo de red NTP, listas de control de acceso ACL.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Utilizar herramientas de simulación para establecer escenarios LAN/WAN los cuales permitan realizar un análisis sobre el comportamiento de los diversos protocolos y métricas de enrutamiento que se requieren en la configuración e implementación de la red planteada para los dos entornos corporativos planteados bajo el uso de la tecnología CISCO

2.2 OBJETIVOS ESECIFICOS

1. Identificar las herramientas de supervisión y protocolos de administración de una red
2. Evaluar el desempeño de routers y switches
3. Usar comandos especializados en gestión de redes
4. Diseñar políticas de enrutamiento dinámico con OSPF
5. Proporcionar conectividad, seguridad y acceso a la WAN mediante protocolo DHCP,NAT y LCA

DESARROLLO

ESCENARIO 1

Topología

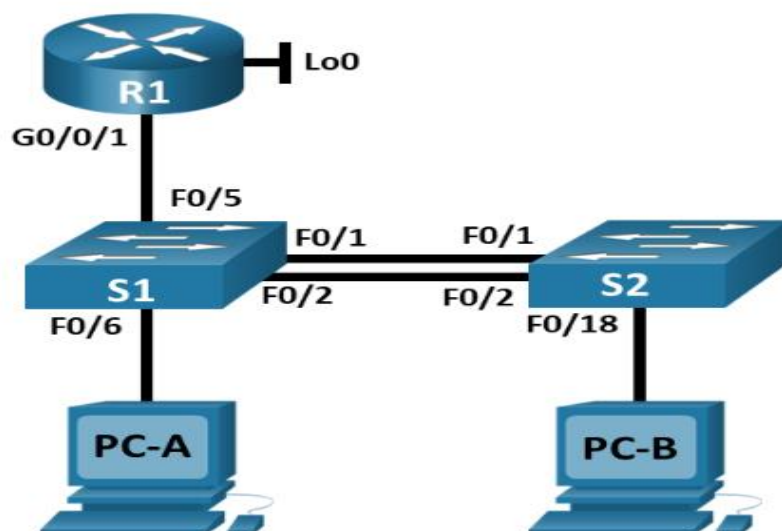


Tabla 1 VLAN Escenario 1

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla de asignación de direcciones

Tabla 2 Asignación de direcciones IP Escenario 1

Dispositivo/Interface	Dirección IP/Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1/26	No corresponde
	2001:db5:acad:a::1/64	No corresponde
R1 G0/0/1.3	10.21.5.65/27	No corresponde
	2001:db5:acad:b::1/64	No corresponde
R1 G0/0/1.4	10.21.5.97/29	No corresponde
	2001:db5:acad:c::1/64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1/27 2001:db8:acad:209::1/64	No corresponde
S1 VLAN 4	10.21.5.98/29	10.21.5.97
	2001:db5:acad:c::99/64	No corresponde
	fe80::98	No corresponde
S2 VLAN 4	10.21.5.99/29	10.21.5.97
	2001:db5:acad:c::99 /64	No corresponde
	fe80::99	No corresponde
PC A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:a::50 /64	fe80::1
PC B NIC	DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:b::50 /64	fe80::1

Instrucciones

Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

Paso 1: Inicializar y volver a cargar el Router y el switch

Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

Comandos usados para Inicializar y recargar R1

Router R1

Router>enable

Router# erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue?confirm

OK

Erase of nvram:complete

Router#delete vlan.dat

Delete filename vlan.dat? confirm

Delete flash:/vlan.dat? confirm

No such file or directory

Router #reload

Proceed with reload? Confirm

System configuration has been modified.save? yes/ no :yes

Comandos usados para Inicializar y recargar S1

Switch S1

Switch>

Switch>enable

Switch# delete vlan.dat

Delete filename vlan.dat?

Confirm

Switch# erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue confirm

OK

Erase of nvram:complete

Switch # reload

Proceed with reload? Confirm

System configuration has been modified.save? yes/ no : yes

Comandos usados para Inicializar y recargar S2

Switch S2

```
Switch>
Switch>enable
Switch# delete vlan.dat
Delete filename vlan.dat?
Confirm
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue confirm
OK
Erase of nvram:complete
Switch # reload
Proceed with reload? Confirm
System configuration has been modified.save? yes/ no :yes
```

Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

Switch S1

```
Switch>
Switch>enable
Switch# config t
Switch(config)# sdm prefer dual -ipv4-and-ipv6 default
Switch(config)# end
Switch#reload
System configuration has been modified.save? yes/ no :yes
Building configuration.
ok
```

Switch S2

```
Switch>
Switch>enable
Switch# configure t
Switch(config)# sdm prefer dual -ipv4-and-ipv6 default
Switch(config)# end
Switch#reload
System configuration has been modified.save? yes/ no :yes
Building configuration.
Ok
```

Paso 2: Configure R1

Tabla 3 Configuración R1

Tarea	Especificaciones
Desactivar la búsqueda DNS	No IP domain-lookup
Nombre del router	Hostname R1
Nombre de dominio	ccna-lab.com ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass Enable secret ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass Line console 0 Password ciscoconpass login
Establecer la longitud mínima para las contraseñas	10 caracteres Security password min-leng 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass Username admin password admin 1 pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vty 0 15 login local
Configurar VTY solo aceptando SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configure un MOTD Banner	Banner motd " Ingreso solo para personal autorizado"
Habilitar el routing IPv6	Ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterface	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80::1 Establece la dirección IPv6. Activar la interfaz .Int g0/0/1.2 Encapsulation dot1q 2 Description BIKES

	Ip address 10.21.5.1 255.255.255.192 Ipv6 address 2001:db5:acad:a:1/64 Ipv6 address fe80::1 link local Int g0/0/1.2 No shutdown Int g0/0/1.3 Encapsulation dot1q 3 Description TRIKES Ip address 10.21.5.65 255.255.255.224 Ipv6 address 2001:db5:acad:b:1/64 Ipv6 address fe80::1 link local Int g0/0/1.4 Encapsulation dot1q 4 Description MANAGEMENT Ip address 10.21.5.97 255.255.255.248 Ipv6 address 2001:db5:acad:c:1/64 Ipv6 address fe80::1 link local Int g0/0/1.6 Encapsulation dot1q 6 Description NATIVE No shutdown
Configure elLoopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1 Interface loopback 0 Ip address 209.165.201.1 255.255.255.224 Ipv6 address 2001:db8:acad:209::1/64 Ipv6 address fe80::1 link-local Description INTERNET
Generar una clave de cifrado RSA	Módulo de 1024bits crypto key generate rsa modulus 1024

Comandos usados para configuración R1

```

Router>
Router>enable
Router# config t

```

```

Router(config)# no ip domain-lookup
Router(config)# hostname R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line con 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security password min-length 10
R1(config)#username admin privilege 15 secret admin1pass
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd "Acceso solo personal Autorizado"

```

Comandos usados para configurar interfaces

```

R1(config)#ipv6 unicast-routing
R1(config)#interface g0/0/1.2
R1(config-if)#int g0/0/1.2
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#description vlan BIKES
R1(config-subif)#ip address 10.21.5.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db5:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit

R1(config)#interface g0/0/1.3
R1(config-if)#int g0/0/1.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#description vlan Trikes
R1(config-subif)#ip address 10.21.5.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db5:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit

```

```
R1(config)#interface g0/0/1.4
R1(config-if)#int g0/0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#description vlan Management
R1(config-subif)#ip address 10.21.5.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db5:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
R1(config)#interface g0/0/1.5
R1(config-if)#int g0/0/1.5
R1(config-subif)#encapsulation dot1Q 5
R1(config-subif)#description Parking
R1(config-subif)#exit
R1(config)#interface g0/0/1.6
R1(config-if)#int g0/0/1.6
R1(config-subif)#encapsulation dot1Q 6
R1(config-subif)#description Native
R1(config-subif)#exit
```

```
R1(config)#interface g0/0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
```

```
R1(config)#interface g0/0/1
R1(config-if)#no shutdown
```

```
R1#config t
R1(config)#interface loopback 0
```

```
R1(config-if)#ip address 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 address 2001:db5:acad:209::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#exit
```

Comandos usados para clave cifrado rsa

```
R1(config)#crypto key generate rsa
general-key modulus 1024
R1(config)#
```

Paso 3: Configure S1 y S2.

Tabla 4 configuración S1 y S2

Tarea	Especificaciones
Desactivar la búsqueda DNS.	No ip domain lookup
Nombre del switch	S1 o S2, según proceda Hostname S1 Hostname S2
Nombre de dominio	ccna-lab.comip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	CiscoenpassEnable secret ciscoenpass
Contraseña de acceso a la consola	CiscoconpassLine console 0Password ciscoconpassLogin
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass Username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vty 0 15Login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Transportinput ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	Banner motd "Acceso solo para personal autorizado"
Generar una clave de cifrado RSA	Módulo de 1024bits Crypto key generate rsa modulus 10242
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3 Int vlan 4 Ip address 10.19.8.98 255.255.255.248 Ipv6 address 2001:db5:acad:c::98/64 Ipv6 address fe80::98 link-local Description MANAGEMENT No shutdown
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4 Ip Default-gateway 10.21.5.97

Comandos usados para configuración S1

```
Switch>
switch>enable
switch# config t
switch(config)# no ip domain-lookup
switch(config)# hostname S1
S1(config)#ip domain-name ccna-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line con 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin privilege 15 secret admin1pass
S1(config)#line vty 0 4
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd "Acceso solo personal Autorizado
S1(config)#crypto key generate rsa
general-key modulus 1024
S1(config)#
```

Comandos usados para configuración S2

```
Switch>
switch>enable
switch# config t
switch(config)# no ip domain-lookup
switch(config)# hostname S2
S2(config)#ip domain-name ccna-lab.com
S2(config)#enable secret ciscoenpass
S2(config)#line con 0
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit
S2(config)#username admin privilege 15 secret admin1pass
S2(config)#line vty 0 4
S2(config-line)#login local
S2(config-line)#transport input ssh
```

```

S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd "Acceso solo personal Autorizado
S2(config)#crypto key generate rsa
general-key modulus 1024
S2(config)#

```

Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Paso 4: Configurar S1

Tabla 5 configuración S1

Tarea	Especificaciones
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4,nombre Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apaga

Comandos usados para configuración VLAN en S1

```

S1>enable
S1# config t
S1(config)# vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#vlan 4
S1(config-vlan)#name Management

```

```
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#
```

Comandos usados para configuración Trunking en S1 con vlan 6 Nativa

```
S1>enable
S1# config t
S1(config)#interface f0/1
S1(config-if)#switchport trunk encapsulation dot1Q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#no sh
S1(config-if)#exit
S1(config)#
```

```
S1(config)#interface f0/2
S1(config-if)#switchport trunk encapsulation dot1Q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#no sh
S1(config-if)#exit
S1(config)#
```

```
S1(config)#interface f0/5
S1(config-if)#switchport trunk encapsulation dot1Q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#no sh
S1(config-if)#exit
S1(config)#
```

Comandos usados para configuración grupo de puertos EtherChannel Con interfaces f0/1 y f0/2 con protocolo LACP

```
S1>enable
S1# config t
S1(config)#interface rang f0/1-2
S1(config-if-range)#channel-protocol lacp
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#exit
S1(config-if)#exit
S1(config)#
```

Comandos usados para configuración del puerto de acceso de host para VLAN 2 interface f0/6

```
S1>enable
S1# config t
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport acces vlan 2
S1(config-if)#exit
S1(config)#
```

Comandos usados para configuración de seguridad del puerto en los puertos de acceso con 3 direcciones MAC

```
S1>enable
S1# config t
S1(config)#interface range f0/1-2,f0/5-6
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#switchport port-security maximum 3
S1(config-if-range)#exit
S1(config)#
```

Comandos usados para configuración de protección de todas las interfaces no utilizadas asignadas a VLAN 5

```
S1# config t
S1(config)#interface range f0/3-4,f0/7-24
S1(config-if-range)#switchport mode access
```

```

S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#shutdown
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#exit
S1(config)#

```

Paso 5: Configure el S2

Tabla 6 configuración S2

Tarea	Especificaciones
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, nombre Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 3	Interfaces F0/18
Configurar la seguridad del puerto en los puertos de acceso	permite 3 MAC addresses
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Comandos usados para configuración VLAN en S2

```

S2>enable
S2# config t
S2(config)# vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#vlan 4
S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native
S2(config-vlan)#exit

```

S2(config)#

Comandos usados para configuración Trunking en S2 con vlan 6 Nativa

```
S2>enable
S2# config t
S2(config)#interface f0/1
S2(config-if)#switchport trunk encapsulation dot1Q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#no sh
S2(config-if)#exit
S2(config)#
```

```
S2(config)#interface f0/2
S2(config-if)#switchport trunk encapsulation dot1Q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#no sh
S2(config-if)#exit
S2(config)#
```

Comandos usados para configuración grupo de puertos EtherChannel Con interfaces f0/1 y f0/2 con protocolo LACP

```
S2>enable
S2# config t
S2(config)#interface rang f0/1-2
S2(config-if-range)#channel-protocol lacp
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#exit
S2(config-if)#exit
S2(config)#
```

Comandos usados para configuración del puerto de acceso de host para VLAN 3 interface f0/18

```
S2>enable
S2# config t
```

```

S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport acces vlan 3
S2(config-if)#exit
S2(config)#

```

Comandos usados para configuración de seguridad del puerto en los puertos de acceso con 3 direcciones MAC

```

S2>enable
S2# config t
S2(config)#interface range f0/1-2,f0/18
S2(config-if-range)#switchport port-security mac-address sticky
S2(config-if-range)#switchport port-security maximum 3
S2(config-if-range)#exit
S2(config)#

```

Comandos usados para configuración de protección de todas las interfaces no utilizadas asignadas a VLAN 5

```

S2# config t
S2(config)#interface range f0/3-17,f0/19-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#shutdown
S2(config-if-range)#switchport port-security violation shutdown
S2(config-if-range)#exit
S2(config)#

```

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Tabla 7 configuración R1

Tarea	Especificaciones
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
ConfigurarIPv4DHCPpara VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente.

	Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Comandos usados para configuración R1 por defecto

```
R1>enable
R1#conf t
R1(config)#ip route 0.0.0.00.0.0.0 loopback 0
R1(config)#ipv6 route ::/0 loopback 0
```

Comandos usados para configuración IPv4 DHCP para VLAN 2

```
R1(config)#ip dhcp excluded-address 10.21.5.1 10.21.5.52
R1(config)#ip dhcp pool vlan2-Bikes
R1(dhcp-config)# net 10.21.5.0 255.255.255.192
R1(dhcp-config)# default-router 10.21.5.1
R1(dhcp-config)# domain-name ccna-a.net
R1(dhcp-config)# exit
```

Comandos usados para configuración IPv4 DHCP para VLAN 3

```
R1(dhcp-config)# ip dhcp excluded-address 10.21.5.65 10.21.5.84
R1(config)#ip dhcp pool vlan3-Trikes
R1(dhcp-config)# net 10.21.5.64 255.255.255.224
R1(dhcp-config)# default-router 10.21.5.65
R1(dhcp-config)# domain-name ccna-b.net
R1(dhcp-config)# exit
R1(config)#do wr
```


Paso 2: Configurar los servidores

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 8 configuración Servidores

PC-A Network configuration	
Descripción	Comando ipconfig /all
Dirección física	000D.BDED.E316
Dirección IP	10.21.5.40
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.53
Gateway predeterminado IPv6	FE80::1

PC-B Network configuration	
Descripción	Comando ipconfig /all
Dirección física	0001.642C.6293
Dirección IP	10.21.5.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

Parte 3: Probar y verificar la conectividad de extremo a extremo

Tabla 9 Realizando Ping de extremo a extremo

Desde	A	De Internet	IP	Resultado
PC-A	R1,G0/0/1.2	Dirección	10.21.5.1	Positivo
		IPV6	2001:db5:acad:a::1	Positivo
	R1,G0/0/1.3	Dirección	10.21.5.65	Positivo
		IPV6	2001:db5:acad:b::1	Positivo
	R1,G0/0/1.4	Dirección	10.21.5.97	Positivo
		IPV6	2001:db5:acad:c::1	Positivo
	S1,VLAN 4	Dirección	10.21.5.98	Positivo
		IPV6	2001:db5:acad:c::98	Negativo
	S2,VLAN 4	Dirección	10.21.5.99	Positivo
		IPV6	2001:db5:acad:c::99	Negativo
	PC-B	Dirección	IP address will vary	Positivo
		IPV6	2001:db5:acad:b::50	Positivo

PC-B	R1 Bucle 0	Dirección	209.165.201.1	Positivo
		IPV6	2001:db5:acad:209::1	Positivo
	R1 Bucle 0	Dirección	209.165.201.1	Positivo
		IPV6	2001:db5:acad:209::1	Positivo
	R1,G0/0/1.3	Dirección	10.21.5.65	Positivo
		IPV6	2001:db5:acad:B:1	Positivo
	R1,G0/0/1.4	Dirección	10.21.5.97	Positivo
		IPV6	2001:db5:acad:C:1	Positivo
	S1,VLAN 4	Dirección	10.21.5.98	Positivo
		IPV6	2001:db5:acad:C:98	Negativo
	S2,VLAN 4	Dirección	10.21.5.99	Positivo
		IPV6	2001:db5:acad:C:99	Negativo

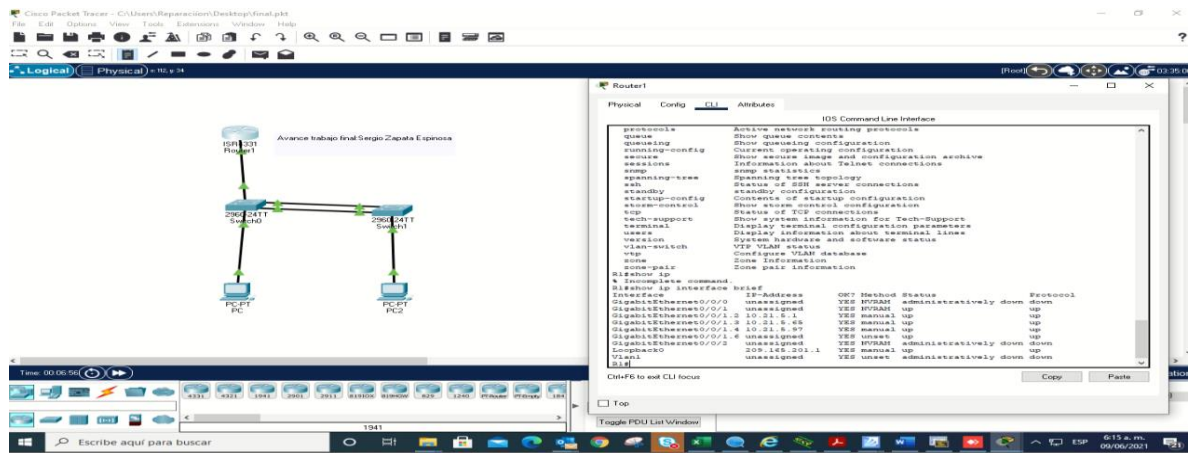


Figura 1. Show ip Interface brief de mi propia autoría

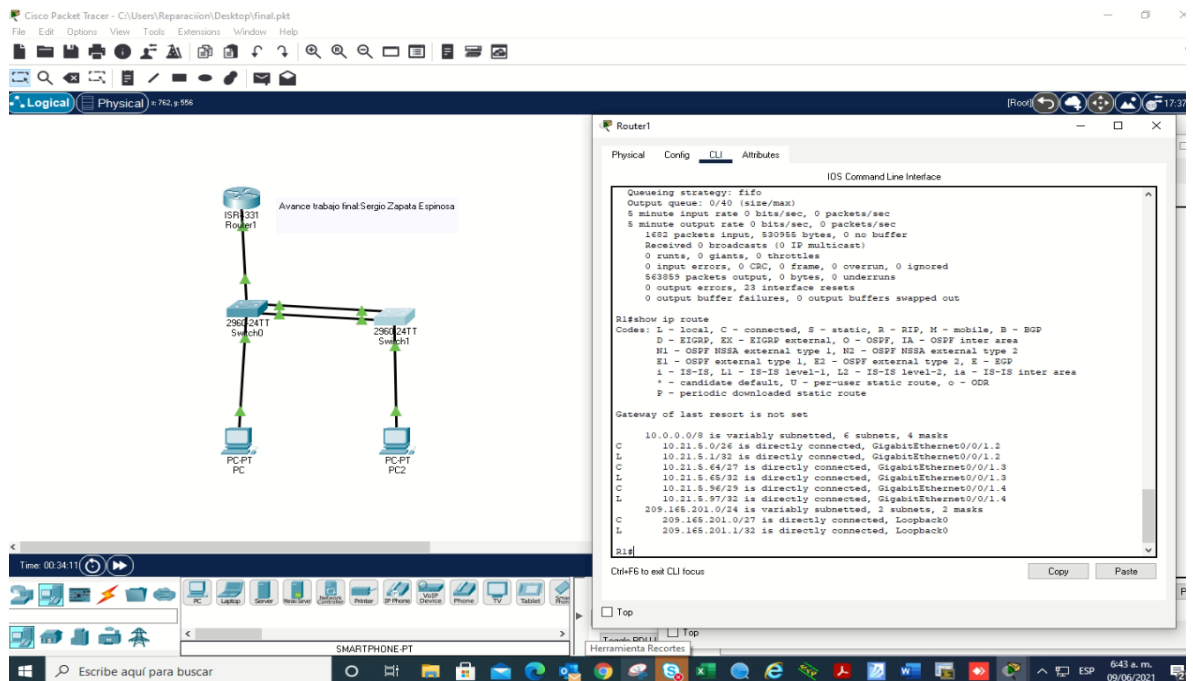


Figura 2.show ip route de mi propia autoría

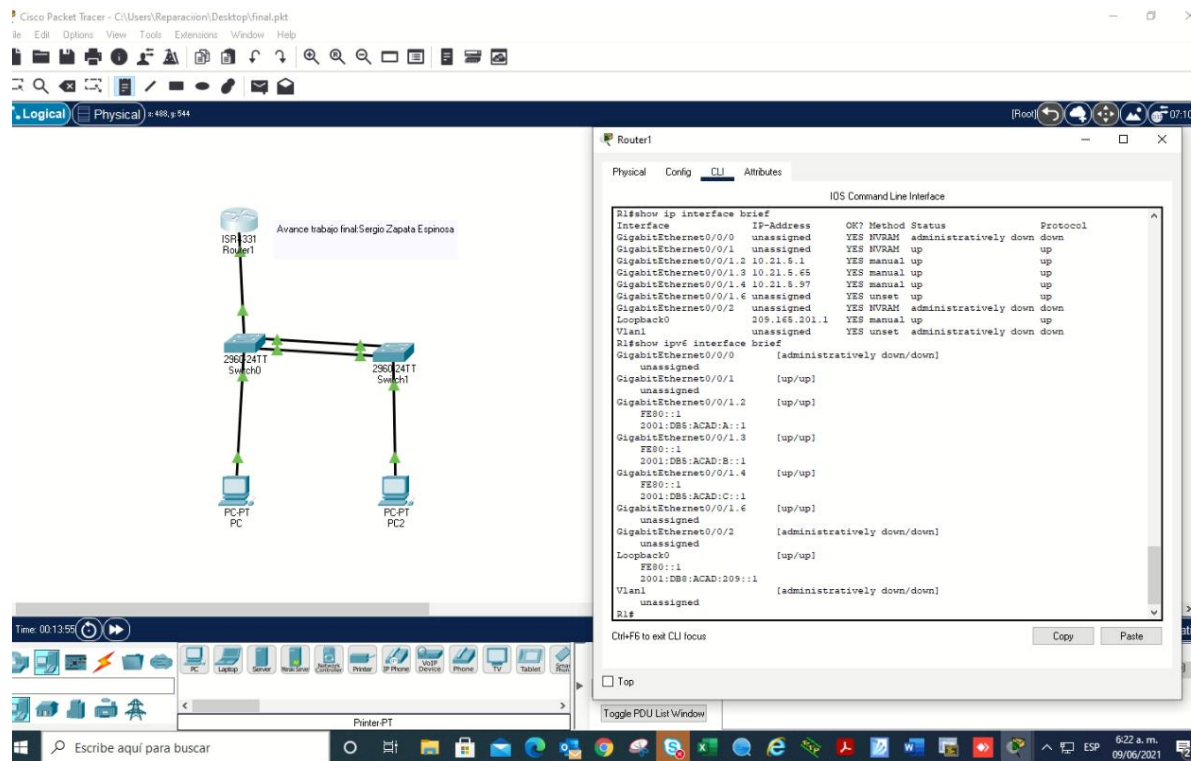


Figura 3.show ipv6 interface brief de mi propia autoría

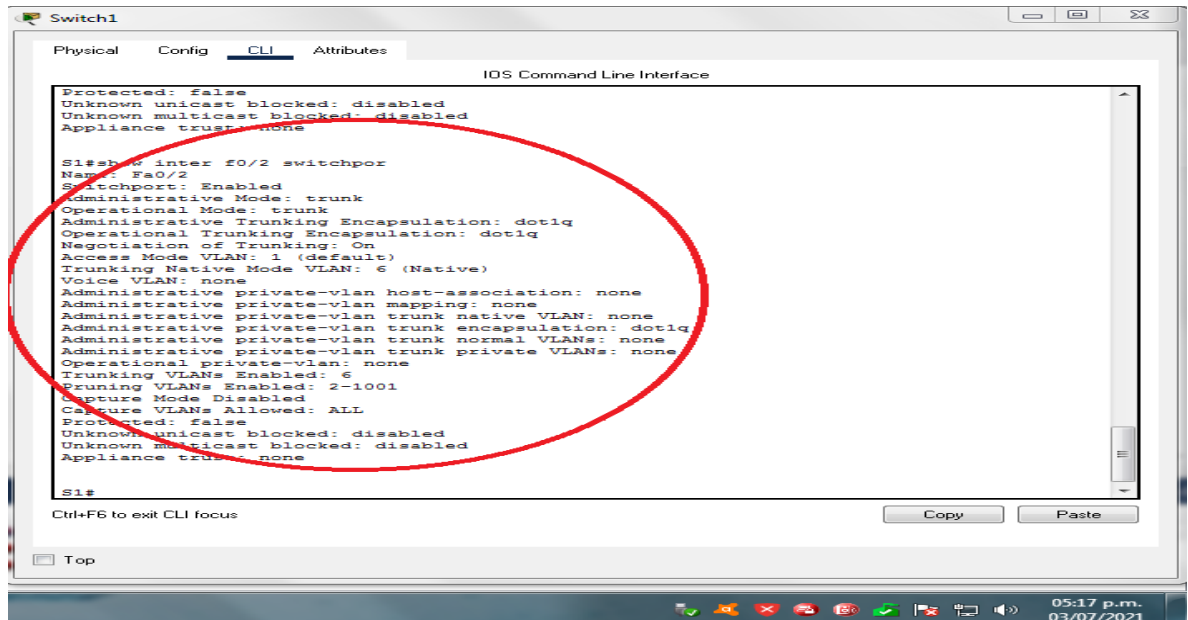


Figura 6. Show inter f0/2 switchport de mi propia autoría

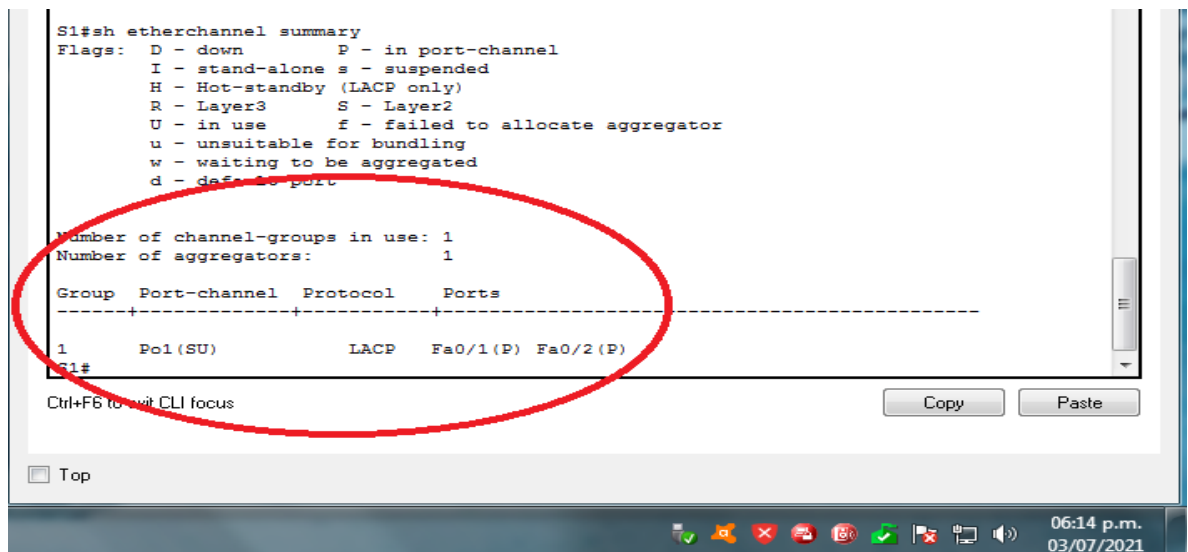


Figura 7. Show etherchanel summary

```
Si#sh etherchannel port-channel
Channel-group listing:
-----
Group: 1
-----
Port-channels in the group:
-----
Port-channel: Po1 (Primary Aggregator)
-----
Age of the Port-channel = 00d:01h:08m:09s
Logical slot/port = 2/1 Number of ports = 2
GC = 0x00000000 HotStandBy port = null
Port state = Port-channel
Protocol = LACP
Port Security = Disabled

Ports in the Port-channel:
-----
Index Load Port EC state No of bits
-----
0 00 Fa0/1 Active 0
1 00 Fa0/2 Active 0
Time since last port bundled: 00d:00h:10m:03s Fa0/2
Si#
Si#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

06:20 p.m. 03/07/2021

Figura 8. Show etherchannel port-channel de mi propia autoría

```
Si#sh vlan brief
-----
VLAN Name Status Ports
-----
1 default active Fa0/6
2 Bikes active Fa0/6
3 Trikes active Fa0/6
4 Management active Fa0/6
5 Parking active Fa0/6, Fa0/4, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gig0/1, Gig0/2
6 Native active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Si#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ES 06:43 p.m. 03/07/2021

Figura 9. Show vlan brief de mi propia autoría


```

0.0.0.0
C:\>
C:\>ping 10.21.5.1
Pinging 10.21.5.1 with 32 bytes of data:
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Ping statistics for 10.21.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.21.5.65
Pinging 10.21.5.65 with 32 bytes of data:
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Ping statistics for 10.21.5.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.21.5.97
Pinging 10.21.5.97 with 32 bytes of data:
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Ping statistics for 10.21.5.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Figura 12.Haciendo ping de PC-A de mi propia autoría

```

Pinging 10.21.5.98 with 32 bytes of data:
Reply from 10.21.5.98: bytes=32 time=16ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Ping statistics for 10.21.5.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 4ms
C:\>ping 10.21.5.99
Pinging 10.21.5.99 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Ping statistics for 10.21.5.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.21.5.99
Pinging 10.21.5.99 with 32 bytes of data:
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Ping statistics for 10.21.5.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>

```

Figura 13.Haciendo ping de PC-B de mi propia autoría


```

S1#sh etherchannel port-channel
Channel-group listing:
-----
Group: 1
-----
Port-channels in the group:
-----
Port-channel: Po1 (Primary Aggregator)
-----
Age of the Port-channel = 00d:01h:08m:09s
Logical slot/port = 2/1 Number of ports = 2
GC = 0x00000000 HotStandBy port = null
Port state = Port-channel
Protocol = LACP
Port Security = Disabled

Ports in the Port-channel:
-----
Index Load Port EC state No of bits
-----
0 00 Fa0/1 Active 0
1 00 Fa0/2 Active 0
Time since last port bundled: 00d:00h:10m:03s Fa0/2
S1#
S1#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

06:20 p.m.
03/07/2021

Figura 14. Protocolo LACP de mi propia autoría

Escenario 2

Topología

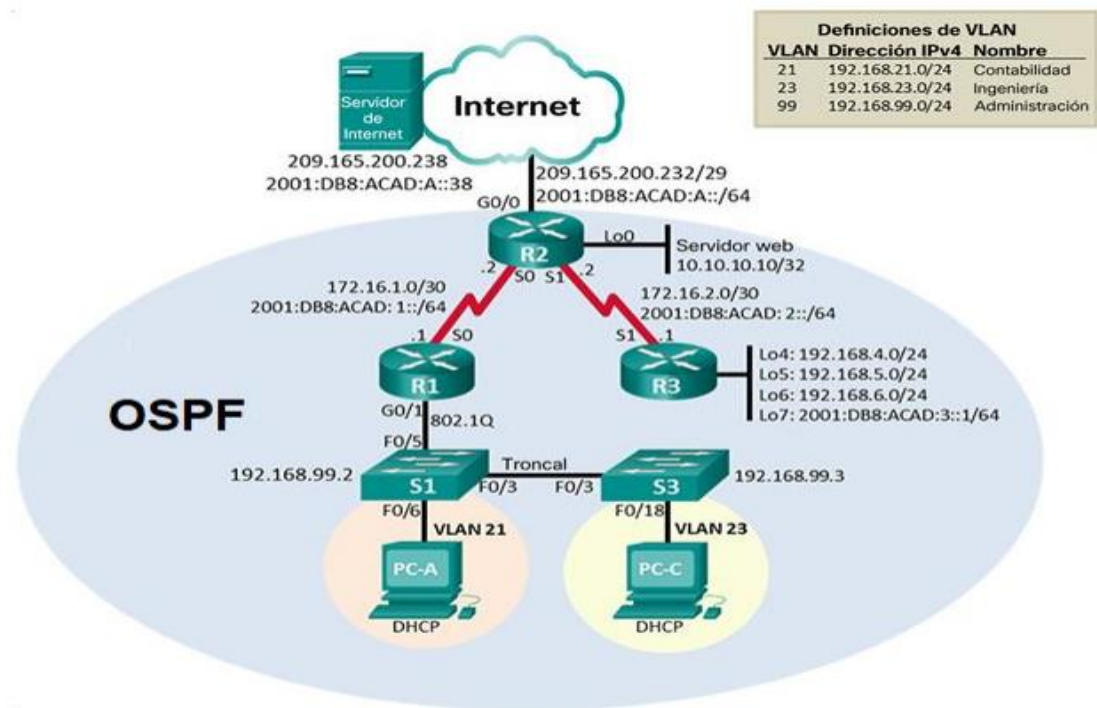


Figura:

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

Tabla 10 inicializando router y switch Escenario 2

Tarea	Comandos de IOS
Eliminar el archivo startup-config de todos los routers	router1# erase startup-config router2# erase startup-config router3# erase startup-config
Volver a cargar todos los router	router1# reload router2# reload router3# reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch1# erase startup-config Erase of nvram:complete Switch3#erase startup-config Erase of nvram:complete Switch1#delete vlan.dat Switch3#delete vlan.dat
Volver a cargar ambos switches	switch1# reload Switch3# reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	switch1# show flash Switch2# show flash

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Tabla 11 configurando PC internet Escenario 2

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 12 configuración básica R1 Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	router(config)#no ip domain-lookup
Nombre del router	router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login

Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	banner motd "Se prohíbe el acceso no autorizado."
Interfaz S0/0/0 Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz	R1(config)#interface s0/0/0 R1(config)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#no shutdown R1(config-if)#description link-R1-R2 R1(config-if)#clock rate 128000 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#no shutdown
Rutas predeterminadas Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0	R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1(config)#ipv6 route ::/0 2001:db8:acad:1:2

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 13configuración básica R2 Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	router#conf t router(config)#no ip domain-lookup
Nombre del router	router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line con 0 R2(config- line)#password cisco
Contraseña de acceso Telnet	R2(config-line)#line vty 0 4 R2(config- line)#password cisco
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2#conf t R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd " Se prohíbe el acceso no autorizado. "

<p>Interfaz S0/0/0</p> <p>Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz</p>	<pre>R2(config)#int s0/0/0 R2(config-if)#ip add 172.16.1.2 255.255.255.252 R2(config-if)#no shutdown R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown R2(config-if)#description link-R2-R1</pre>
<p>Interfaz S0/0/1</p> <p>Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz</p>	<pre>R2(config)#int s0/0/1 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#no shutdown R2(config-if)#clock rate 128000 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#description link-R2-R3</pre>
<p>Interfaz G0/0 (simulación de Internet)</p> <p>Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz</p>	<pre>R2(config)#INT G0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config)#no shutdown R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#</pre>
<p>Interfaz loopback 0 (servidor web simulado)</p> <p>Establecer la descripción. Establezca la dirección IPv4</p>	<pre>R2(config)#int lo0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config)#no shutdown</pre>
<p>Ruta predeterminada</p> <p>Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0</p>	<pre>R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.238 R2(config)#ipv6 route ::/0 2001:db8:acad:a::38</pre>

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 14configuración básica R3 Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class R3(config)#line console 0
Contraseña de acceso a la consola	R3(config-line)#password cisco R3(config)#line vty 0 4
Contraseña de acceso Telnet	R3(config-line)#password cisco
Cifrar las contraseñas de texto no	R3(config)#service password-

cifrado	encryption
Mensaje MOTD	R3(config)#banner motd "Se prohíbe el acceso no autorizado"
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred . Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R3(config)#int s0/0/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#no shutdown R3(config-if)#description link-R2-R3 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config)#no shutdown
Interfaz loopback 4 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#int lo4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred	R3(config)#int lo5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#int lo6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones	R3(config)#int lo7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 R3(config)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 15configuración básica S1 Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)# no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class S1(config)#line con 0
Contraseña de acceso a la consola	S1(config-line)#password cisco S1(config-line)#line vty 0 4
Contraseña de acceso Telnet	S1(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd "Se prohíbe el acceso no autorizado"

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas

Tabla: 16 configuración básica S3 Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)# no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class S3(config)#line con 0
Contraseña de acceso a la consola	S3(config-line)#password cisco S3(config-line)#line vty 0 4
Contraseña de acceso Telnet	S3(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd "Se prohíbe el acceso no autorizado"

Paso 7: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17 Realizando PING entre R1,R2 y PC

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Positivo
R2	R3, S0/0/1	172.16.2.1	Positivo
PC de Internet	Gateway predeterminado	209.165.200.233	Negativo

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 18 Configuración S1 con VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name ingenieria

	S1(config-vlan)#vlan 99 S1(config-vlan)#name administracion
Asignar la dirección IP de administración. Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config)#defaul gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport native vlan1
Forzar el enlace troncal en la interfaz F0/5 Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport native vlan 1
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S1(config)#int range fa0/1-2,fa0/4,fa0/6-24 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#int fa0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#int range fa0/1-2,fa0/4,fa0/7-24 S1(config-if-range)#shutdown

Paso 2:Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 19Configuración S3 con VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN	S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name administracion
Asignar la dirección IP de administración Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado. Asignar la primera dirección IP en la	S3(config)#defaul gateway 192.168.99.1

subred como gateway predeterminado.	
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S3(config)#int fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport native vlan 1
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S3(config)#int range fa0/1-2,fa0/4-24 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config)#int fa0/18 S3(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S3(config)#int range fa0/1-2,fa0/4-17,fa0/19-24 S3(config-if-range)#shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 20

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1 Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.21 R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1 Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.23 R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1 Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config)# no shutdown

Paso 4: Verificar la conectividad de la red Utilice el comando ping para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 21 Realizando PING entre S1 y S3

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Positivo
S3	R1, dirección VLAN 99	192.168.99.1	Positivo
S1	R1, dirección VLAN 21	192.168.21.1	Positivo
S3	R1, dirección VLAN 23	192.168.23.1	Positivo

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22 Configurando OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 10 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	R1(config-router)#network 192.168.99.1 0.0.0.0 area 0 R1(config-router)# network 192.168.23.1 0.0.0.0 area 0 R1(config-router)# network 192.168.21.1 0.0.0.0 area 0 R1(config-router)# network 192.168.1.1 0.0.0.3 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface go/1.21 R1(config-router)# passive-interface go/1.23

	R1(config-router)# passive-interface go/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 23Configurando OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 10 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente Nota: Omitir la red G0/0.	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)# network 172.16.2.0 0.0.0.3 area 0 R2(config-router)# network 10.10.10.10 0.0.0.0 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática	R2(config-router)#no auto-summary

Paso 3:Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 24Configurando OSPF en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 10 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)# network 192.168.4.1 0.0.0.0 area 0 R3(config-router)# network 192.168.5.1 0.0.0.0 area 0 R3(config-router)# network 192.168.6.1 0.0.0.0 area 0

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 25 Utilizando comando sh OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 26 Configurando R1 como servidor DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones	R1(config)#ip dhcp exclude-address 192.168.23.1 192.168.23.20

estáticas	
Crear un pool de DHCP para la VLAN 21. Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#end
Crear un pool de DHCP para la VLAN 23 Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#end

Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 27 Configurando en R2 las NAT

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15	R2(config)#username webuser privilege 15 Password cisco 12345
Habilitar el servicio del servidor HTTP	R1(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R1(config)#ip http authentication local
Crear una NAT estática al servidor web. Dirección global interna: 209.165.200.229	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int loopback 0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#exit

Configurar la NAT dinámica dentro de una ACL privada Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)#access list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access list 1 permit 192.168.6.0 0.0.0.255 R2(config)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit
Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.25.248 R2(config)#exit
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#exit

Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 28 Comprobando protocolos DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ver Imagen
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ver Imagen
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Ver Imagen
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	No reconoce el comando "ip http server"

Parte 6: Configurar NTP

Tabla 29 Configurando NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2# clock set 09:22:00 05 july 2021
Configure R2 como un maestro NTP.	R2# ntp master 5
Configurar R1 como un cliente NTP.	R1#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP	R1(config)#ntp update-calendar R2(config)#exit
Verifique la configuración de NTP en R1.	R1#show ntp associations

Parte 7: Configurar y verificar las listas de control de acceso (ACL)

Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 30 Configurando en R2 ACL y VTY

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 Nombre de la ACL: ADMINMGT	R1(config)#ip access-list standard ADMIN-MGT R1(config-std-nacl)#permit host 172.16.1.1 R1(config-std-nacl)#end
Aplicar la ACL con nombre a las líneas VTY	R1(config)#line vty 0 15 R1(config-line)#access-class ADMIN-MGT in R1(config-line)#transport input telnet
Permitir acceso por Telnet a las líneas de VTY	R1(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 31 Verificando configuración ACL y NAT

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show Access list
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface s0/0/0

<p>¿Con qué comando se muestran las traducciones NAT?</p> <p>Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red</p>	<p>R2#show ip nat translations</p>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<p>R2#clear ip nat translation</p>

```

R2
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up

R2#sh ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        ND - ND Default, NDP - ND Prefix, DCE - Destination, NDR - Redirect
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
C   2001:DB8:ACAD:1::/64 [0/0]
    via Serial0/1/0, directly connected
L   2001:DB8:ACAD:1::2/128 [0/0]
    via Serial0/1/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
    via Serial0/1/1, directly connected
L   2001:DB8:ACAD:2::2/128 [0/0]
    via Serial0/1/1, receive
L   FF00::/8 [0/0]
    via Null0, receive
R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.1.0/30 is directly connected, Serial0/1/0
L       172.16.1.2/32 is directly connected, Serial0/1/0
C       172.16.2.0/30 is directly connected, Serial0/1/1
L       172.16.2.2/32 is directly connected, Serial0/1/1

R2#
  
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

04:18 p.m. 05/07/2021

Figura 15. Show ipv6 route de R2 de mi propia autoría

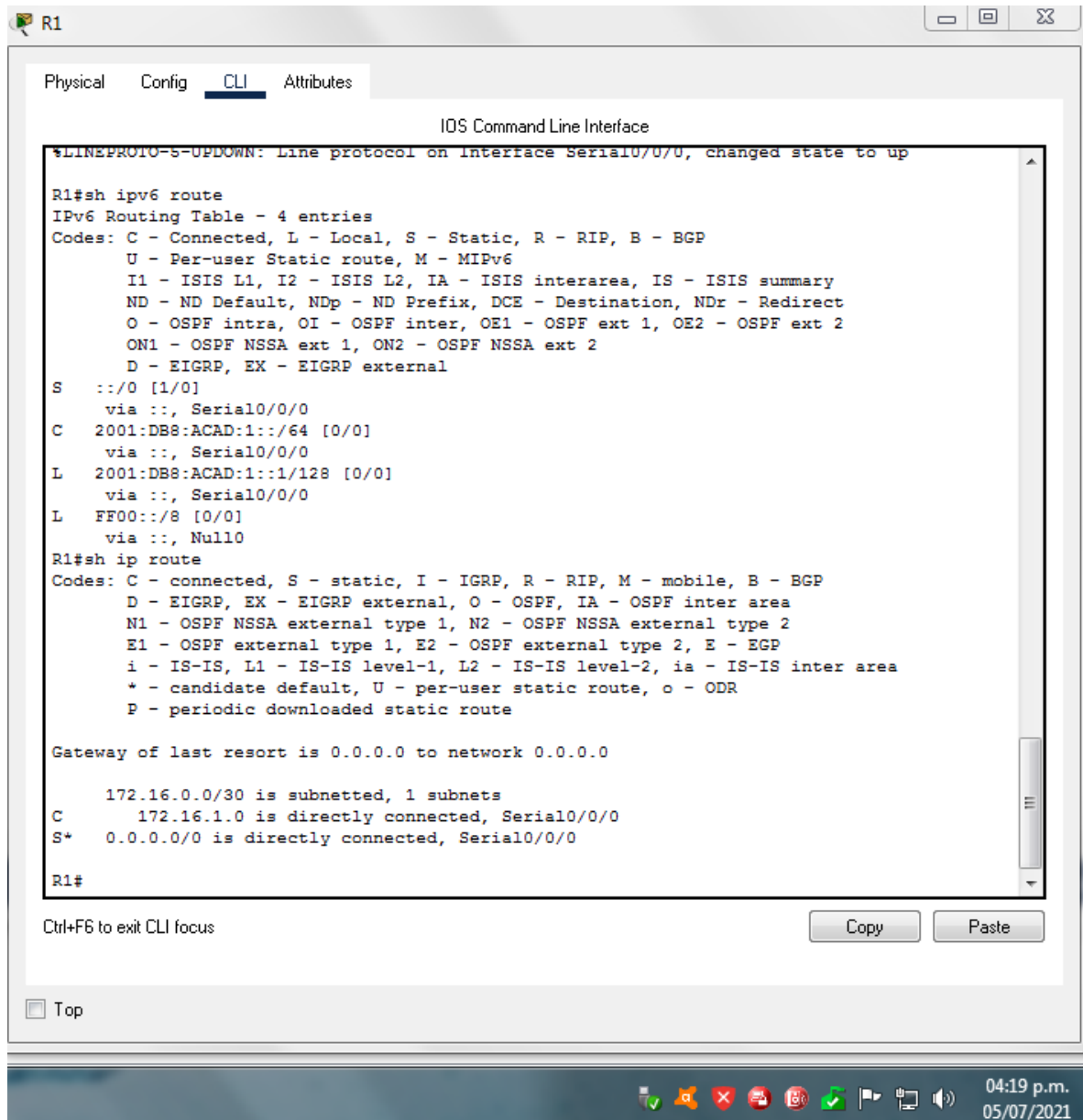


Figura 16. Show ipv6 route de R1 de mi propia autoría

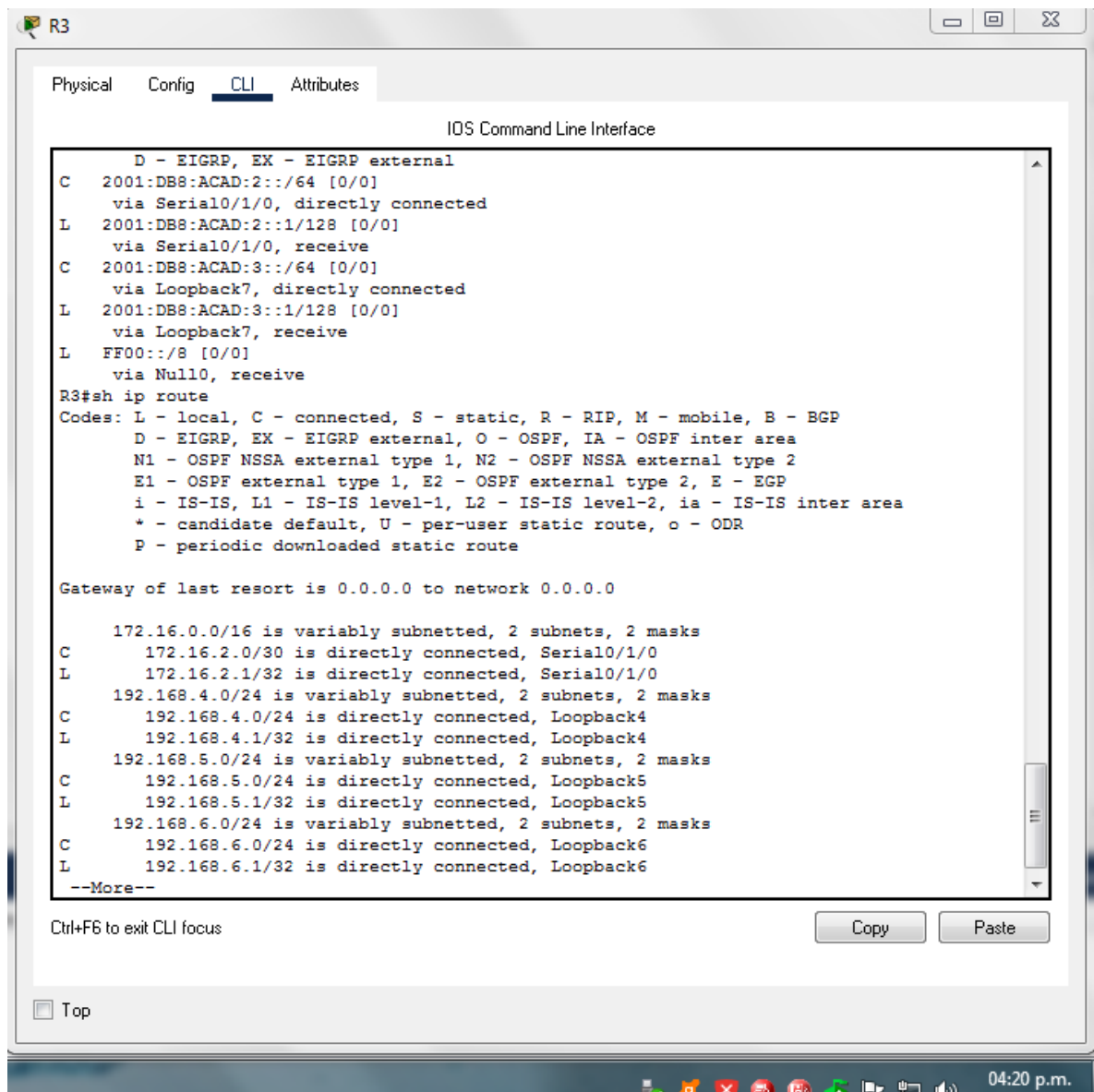


Figura 17. Show ip route de R3 de mi propia autoría

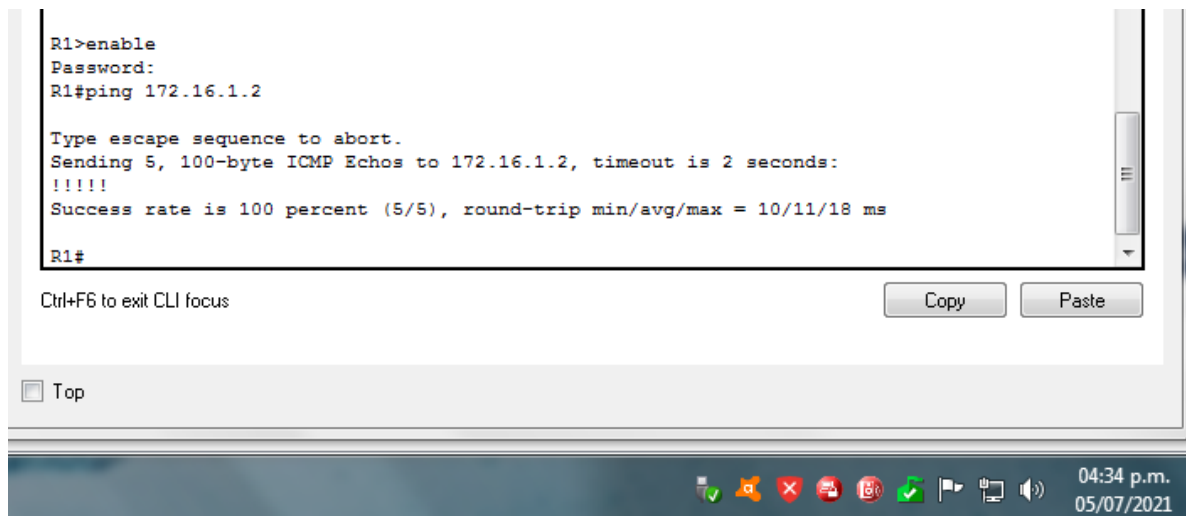


Figura 18. Ping de R1 a R2 de mi propia autoría

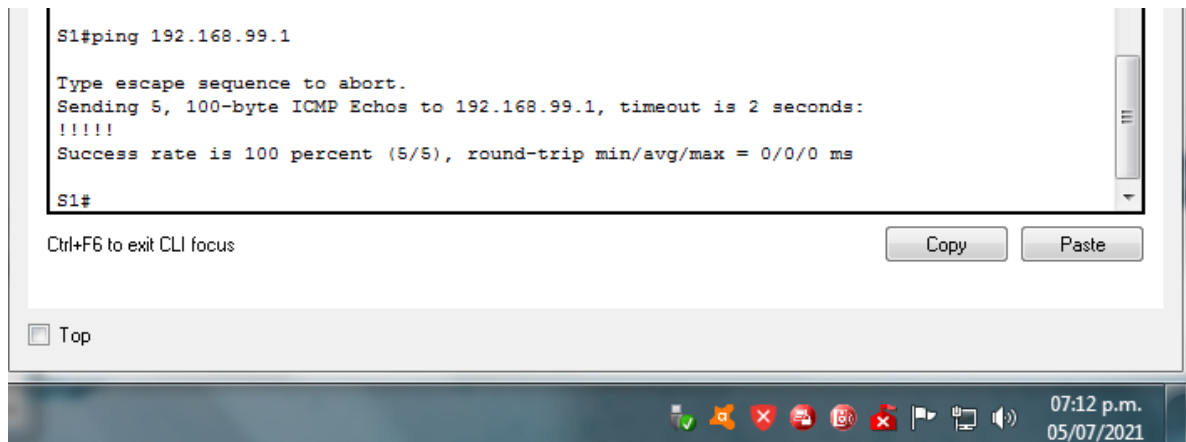


Figura 19. Ping de S1 a S3 de mi propia autoría

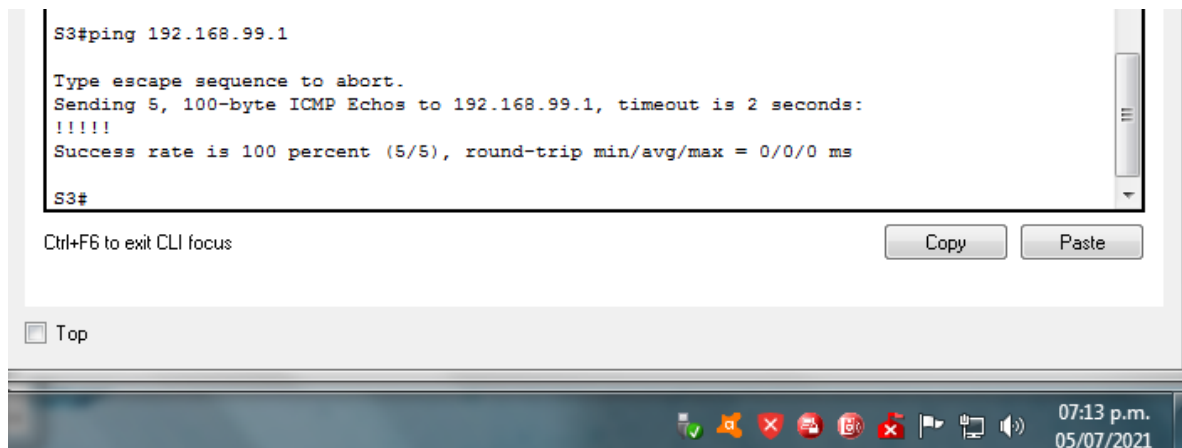


Figura 20.Ping s3 a s2 de mi propia autoría

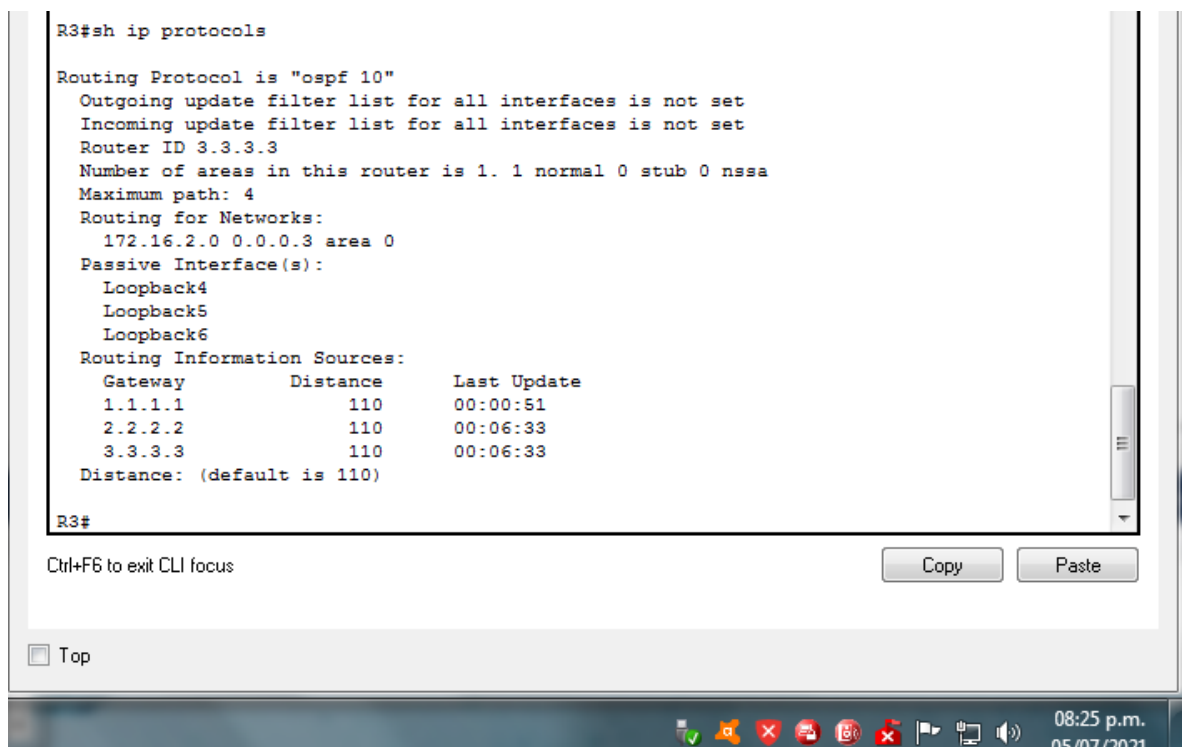


Figura 21.show ip protocols en R3 de mi propia autoría

```
R3#sh ip route ospf
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.1.0 [110/128] via 172.16.2.2, 00:07:19, Serial0/1/0
O      192.168.21.0 [110/129] via 172.16.2.2, 00:07:19, Serial0/1/0
O      192.168.23.0 [110/129] via 172.16.2.2, 00:07:19, Serial0/1/0
O      192.168.99.0 [110/129] via 172.16.2.2, 00:07:19, Serial0/1/0

R3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

08:26 p.m.
05/07/2021

Figura 22.show ip route ospf en R3 de mi propia autoría

```
R3#sh ip ospf
Routing Process "ospf 10" with ID 3.3.3.3
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 2 times
    Area ranges are
      Number of LSA 3. Checksum Sum 0x01d996
      Number of opaque link LSA 0. Checksum Sum 0x000000
      Number of DCbitless LSA 0
      Number of indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0

R3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

08:27 p.m.
05/07/2021

Figura 23.show ip ospf en R3 de mi propia autoría

```
R1#sh ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.99.1
  Number of areas in this router is 0. 0 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.99.1 0.0.0.0 area 0
    192.168.23.1 0.0.0.0 area 0
    192.168.21.1 0.0.0.0 area 0
    172.16.1.0 0.0.0.3 area 0
  Passive Interface(s):
    FastEthernet0/1.21
    FastEthernet0/1.23
    FastEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1           110          00:03:56
    2.2.2.2           110          00:09:39
    3.3.3.3           110          00:09:39
  Distance: (default is 110)
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

08:29 p.m.
05/07/2021

Figura 24.show ip protocols en R1 de mi propia autoría

```
R1#sh ip route ospf
      172.16.0.0/30 is subnetted, 2 subnets
O       172.16.2.0 [110/128] via 172.16.1.2, 00:34:50, Serial0/0/0

R1#sh ip ospf
Routing Process "ospf 1" with ID 192.168.99.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPF's 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0

Routing Process "ospf 10" with ID 1.1.1.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPF's 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 4
    Area has no authentication
    SPF algorithm executed 8 times
    Area ranges are
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

08:31 p.m.
05/07/2021

Figura 25.show ip ospf en R1 de mi propia autoría

```
R1#sh ntp associations

address          ref clock      st  when  poll  reach  delay  offset
disp
~172.16.1.2      127.127.1.1    5   9     16    7     1.00
894511825645.00  0.12
* sys.peer, # selected, + candidate, - outlier, x falseticker, ~ configured
R1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

09:10 p.m.
05/07/2021

Figura 26.show ntp en R1

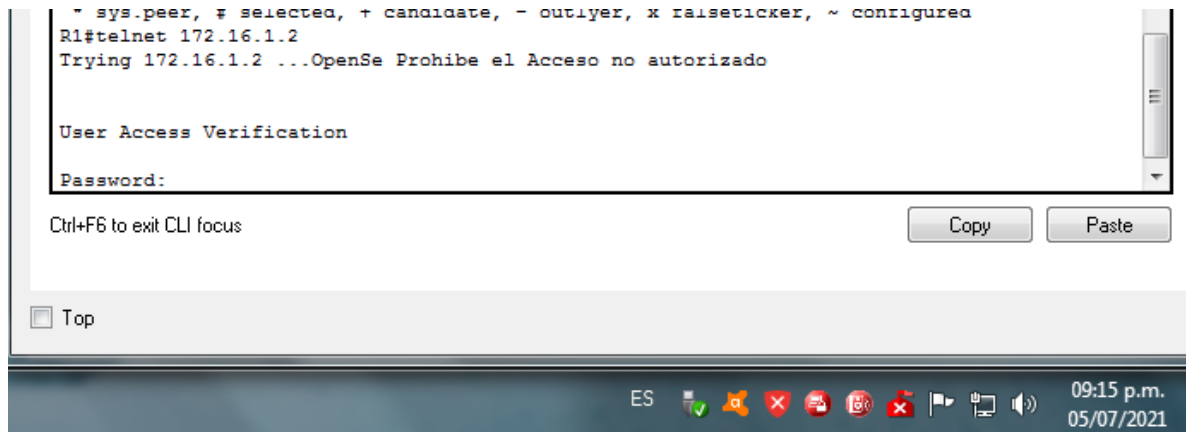


Figura 27.telnet en R1 de mi propia autoría

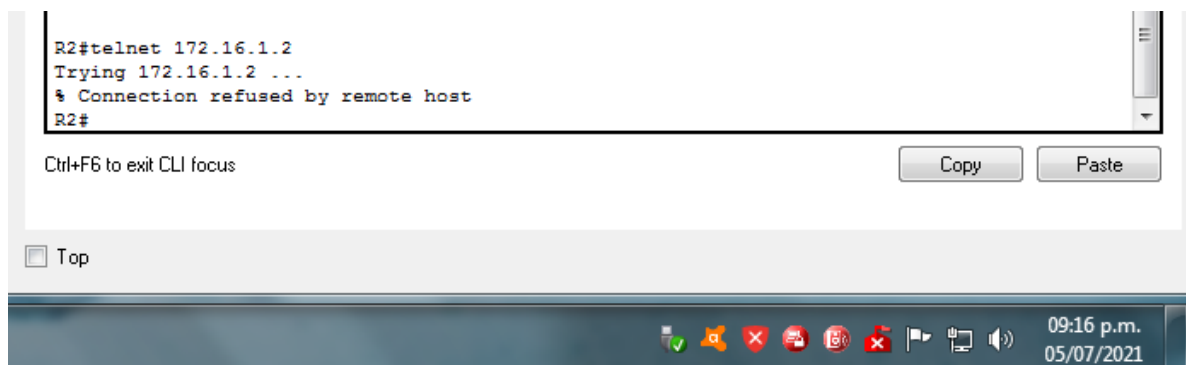


Figura 28.telnet en R2 de mi propia autoría

CONCLUSIONES

En este trabajo realizado basado en dos escenarios logramos mecanizar el proceso de configuración de los router y switchs de una manera rápida, en el primer escenario repasamos los comandos básicos para la configuración de router y switch, como la creación de redes VLAN, asignación de direcciones IPV6, la utilización del software packettracer, asignación de contraseñas, encriptadas de las mismas, configuración DHCP, aunque se nos presentaron varias dificultades por la incompatibilidad del software y el S.O logramos realizar algunas de las actividades solicitadas, adicional para la parte final decidimos cambiar la referencia de los switch 2960 por unos multicapa de referencia 3560

Ya que con los primeros al realizar los diferentes ping de extremo a extremo el resultado fue negativo con todas las direcciones, reconfiguramos varias veces pero la falla persistía por lo tanto y sugerencia de otros compañeros realizamos el cambio obteniendo un mejor resultado aunque en las IPV6 con el PC-A ninguna dio conectividad, sin embargo la experiencia fue bastante positiva porque de la práctica de repetir los comandos nos aprendimos bastantes de ellos.

En el segundo escenario igualmente se nos presentaron dificultades no solo por el corto tiempo para desarrollar la actividad si no que el IOS usado no reconocía los comandos como "ip http server", "no auto-summary" sin embargo el conocimiento adquirido ha sido bastante importante ya que en muchas empresas se ven estos dispositivos por el auge de las telecomunicaciones y la expansión de las diferentes redes, logra tener claro el uso de cada comando que puede ser muy semejante entre otro tipo de marcas con la misma funcionalidad.

BIBLIOGRAFÍA

VESGA, J. Diseño y configuración de redes con Packet Tracer [OVA]. {En línea}.(2014). {25 Noviembre de 2020}. Disponible en:https://1drv.ms/u/s!AmlJYei-NT1lhqCT9VCtl_pLtPD9

CISCO.“Redes Conmutadas. Principios de Enrutamiento y Conmutación”.{En línea}.(2019). {27 Noviembre de 2020}.Disponible en:<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4>

CISCO.“DHCP Principios de Enrutamiento y Conmutación”. {En línea}.(2019). {27 Noviembre de 2020}.Disponible en:<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8>

UNAD. “Configuración de Switches y Routers [OVA]”. {En línea}.(2017). {25 Noviembre de 2020}.Disponible en:<https://1drv.ms/u/s!AmlJYei-NT1lhqL9QChD1m9EuGqC>

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de:<https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5>

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de:
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1>

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de:<https://1drv.ms/u/s!AmlJYei-NT1lhqL9QChD1m9EuGqC>

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de:
<https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6>

Error en Switch 2960 con comando “switchport trunk encapsulation dot1Q”. Recuperado de: <https://community.cisco.com/t5/other-network-architecture/2960-will-not-allow-quot-switchport-trunk-encapsulation-dot1q/td-p/2439012>

ANEXOS

Anexo A. Link Repositorio Handle UNAD.

(Pendiente por aprobación)

Anexo B. Link Articulo IEEE.

<https://drive.google.com/file/d/1pYV1-aglHdgi8MI18zkvHv7RK1dkRN9T/view?usp=sharing>

Anexo C. Link Video Sustentación.

(Pendiente por aprobación)

Estudio de Caso bajo el uso de la tecnología CISCO

(Julio 9 de 2021)

Sergio de J. Zapata Espinosa, szapatae@unadvirtual.edu.co
Universidad Nacional Abierta y a Distancia UNAD

Resumen -Con el presente trabajo se pretende dar a conocer y aprender a utilizar herramientas de simulación como packet tracer con el fin de simular la topología planteada de una pequeña red, igualmente que podamos suministrar información referente a los diferentes comportamientos de las redes LAN y WAN, utilizando los diferentes protocolos y métricas que están establecidas para ellas en su enrutamiento, administración y solución de los diferentes problemas que pueden surgir en la configuración de dispositivos como router, switches y host.

En este escenario específico también se realizarán fuera de las configuraciones básicas generales de los dispositivos antes mencionados las configuraciones referentes a VLAN, DHCP, Etherchannel y post-security.

Palabras clave: Interface, topología, router, switch, host, DCHP, VLAN, métrica.

Abstract

The present work aims to present and learn how to use simulation tools such as packet tracer in order to simulate the proposed topology of a network, also allowing us to provide information regarding the different behaviors of LAN and WAN networks, using the different protocols and metrics that are established for them in their routing, administration and solution of the different problems that may arise in the configuration of devices such as routers, switches and hosts.

In this specific scenario, the configurations referring to VLAN, DHCP, Etherchannel and post-security will also be carried out outside of the general basic configurations of the aforementioned devices.

Keywords: Interface, topology, router, switch, host, DCHP, VLAN, metric

I. Introducción

En este Documento plasmaremos las diferentes configuraciones que se requieren en los dispositivos de una red como lo plantea este estudio de caso referenciándose al escenario 1 del trabajo final como opción de grado al título de ingeniero electrónico, donde partiremos de la configuración básica de cada uno de los dispositivos para luego avanzar en una configuración un poco más compleja que nos garantice conectividad y seguridad teniendo como pilar este último concepto ya que no se puede dejar ninguna posibilidad a que agentes externos logren incursionar en la red establecida generando las consecuencias como hurto de información,

colapso del sistema y las demás que se generan por un ingreso indebido a dicha red.

II. Metodología

Este tipo de investigación se denomina aplicada, ya que el fin es resolver una situación o al menos determinar el origen de las fallas que se presentan y en caso dado de que no se resuelvan justificar el inconveniente presentado, el estudio de caso se basa en una red LAN pequeña, conformada por 2 host, 2 switch y un router, donde uno de los switch con su respectivo PC nos darán indicios de una red diferente pero que ambas se unen por medio de los switch y convergen en un router para una posible salida a internet u otra red pero para el caso de este escenario 1 sólo llegaremos hasta este último dispositivo.

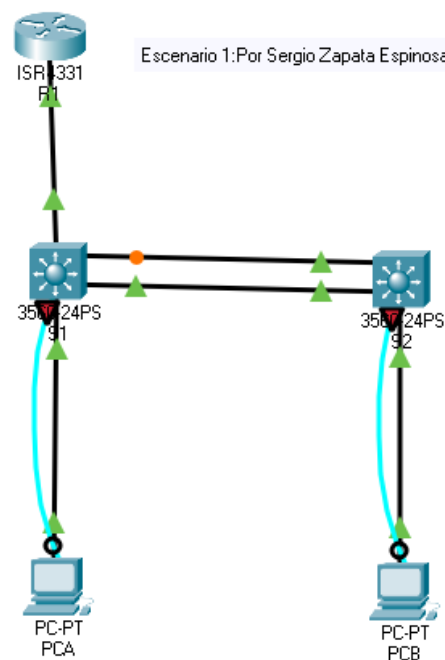


Figura 1. Topología Escenario1, de mi propia autoría

III.Desarrollo

Inicialmente mostramos en la siguiente tabla los nombres correspondientes a las Vlan que se van a crear, igualmente el direccionamiento ip

Tabla 1.Nombre Vlan

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla 2.Asignación de direcciones IP

Dispositivo /Interface	Dirección IP/Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1/26	No corresponde
	2001:db5:acad:a::1/64	No corresponde
R1 G0/0/1.3	10.21.5.65/27	No corresponde
	2001:db5:acad:b::1/64	No corresponde
R1 G0/0/1.4	10.21.5.97/29	No corresponde
	2001:db5:acad:c::1/64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1/27	No corresponde
	2001:db8:acad:209::1/64	No corresponde
S1 VLAN 4	10.21.5.98/29	10.21.5.97
	2001:db5:acad:c::99/64	No corresponde
	fe80::98	No corresponde
S2 VLAN 4	10.21.5.99/29	10.21.5.97
	2001:db5:acad:c::99 /64	No corresponde
	fe80::99	No corresponde
PC A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:a::50 /64	fe80::1
PC B NIC	DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:b::50 /64	fe80::1

En esta primer parte, el objetivo es borrar las posibles configuraciones que puedan tener los dispositivos tanto router como switch para evitar errores de configuración que nos afecten el resultado final de funcionamiento, en otras palabras es colocar el dispositivo en parámetros de fábrica.

A.Comandos Usados para inicializar el router

Router R1

Router>enable

Router# erase startup-config

Erasing the nvram filesystem will remove all configuration files!
Continue? confirm

OK

Erase of nvram:complete

Router#delete vlan.dat

Delete filename vlan.dat? confirm

Delete flash:/vlan.dat? confirm

No such file or directory

Router # reload

Proceed with reload? Confirm

System configuration has been modified.save? yes/ no :yes

B. Comandos usados para Inicializar y recargar S1 Switch S1

Switch>

Switch>enable

Switch# delete vlan.dat

Delete filename vlan.dat?

Confirm

Switch# erase startup-config

Erasing the nvram filesystem will remove all configuration files!
Continue confirm

OK

Erase of nvram:complete

Switch # reload

Proceed with reload? Confirm

System configuration has been modified.save? yes/ no : yes

Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

Switch S1

Switch>

Switch>enable

Switch# config t

Switch(config) # sdm prefer dual -ipv4-and-ipv6 default

Switch(config) # end

Switch#reload

System configuration has been modified.save? yes/ no :yes

Building configuration.

ok

Tabla 3 Configuración R1

Tarea	Especificaciones
Desactivar la búsqueda DNS	No IP domain-lookup
Nombre del router	Hostname R1
Nombre de dominio	ccna-lab.com ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass Enable secret ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass Line console 0 Password ciscoconpass login
Establecer la longitud mínima para las contraseñas	10 caracteres Security password min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass Username admin password admin 1 pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vty 0 15 login local
Configurar VTY solo aceptando SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configure un MOTD Banner	Banner motd “Ingreso solo para personal autorizado”
Habilitar el routing IPv6	Ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterface	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80::1 Establece la dirección IPv6. Activar la interfaz .Int g0/0/1.2 Encapsulation dot1q 2 Description BIKES Ip address 10.21.5.1 255.255.255.192 Ipv6 address 2001:db5:acad:a:1/64 Ipv6 address fe80::1 link local Int g0/0/1.2 No shutdown Int g0/0/1.3 Encapsulation dot1q 3 Description TRIKES Ip address 10.21.5.65 255.255.255.224 Ipv6 address 2001:db5:acad:b:1/64 Ipv6 address fe80::1 link local Int g0/0/1.4 Encapsulation dot1q 4 Description MANAGEMENT Ip address 10.21.5.97 255.255.255.248 Ipv6 address 2001:db5:acad:c:1/64 Ipv6 address fe80::1 link local Int g0/0/1.6 Encapsulation dot1q 6 Description NATIVE No shutdown
Configure el Loopback 0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1 Interface loopback 0 Ip address 209.165.201.1 255.255.255.224 Ipv6 address

	2001:db5:acad:209::1/64 Ipv6 address fe80::1 link-local Description INTERNET
Generar una clave de cifrado RSA	Módulo de 1024bits crypto key generate rsa modulus 1024

Con esta configuración que le damos al router estamos habilitando la seguridad encriptando contraseñas y generando un mensaje de advertencia a usuarios no autorizados y permitiendo accesibilidad con los demás dispositivos en el momento que se configura el direccionamiento IPV4 e IPV6 y todas sus interfaces.

C. Comandos usados para configuración R1

Router>

Router>enable

Router# config t

Router(config)# no ip domain-lookup

Router(config)# hostname R1

R1(config)#ip domain-name ccna-lab.com

R1(config)#enable secret ciscoenpass

R1(config)#line con 0

R1(config-line)#password ciscoconpass

R1(config-line)#login

R1(config-line)#exit

R1(config)#security password min-length 10

R1(config)#username admin privilege 15 secret admin1pass

R1(config)#line vty 0 4

R1(config-line)#login local

R1(config-line)#transport input ssh

R1(config-line)#exit

R1(config)#service password-encryption

R1(config)#banner motd “Acceso solo personal Autorizado”

D. Comandos usados para configurar interfaces

R1(config)#ipv6 unicast-routing

R1(config)#interface g0/0/1.2

R1(config-if)#int g0/0/1.2

R1(config-subif)#encapsulation dot1Q 2

R1(config-subif)#description vlan BIKES

R1(config-subif)#ip address 10.21.5.1 255.255.255.192

```

R1(config-subif)#ipv6 address 2001:db5:acad:a::1/64

R1(config-subif)#ipv6 address fe80::1 link- local

R1(config-subif)#exit

R1(config)#interface g0/0/1.3

R1(config-if)#int g0/0/1.3

R1(config-subif)#encapsulation dot1Q 3

R1(config-subif)#description vlan Trikes

R1(config-subif)#ip address 10.21.5.65 255.255.255.224

R1(config-subif)#ipv6 address 2001:db5:acad:b::1/64

R1(config-subif)#ipv6 address fe80::1 link- local

R1(config-subif)#exit

R1(config)#interface g0/0/1.4

R1(config-if)#int g0/0/1.4

R1(config-subif)#encapsulation dot1Q 4

R1(config-subif)#description vlan Management

R1(config-subif)#ip address 10.21.5.97 255.255.255.248

R1(config-subif)#ipv6 address 2001:db5:acad:c::1/64

R1(config-subif)#ipv6 address fe80::1 link- local

R1(config-subif)#exit

R1(config)#interface g0/0/1.5

R1(config-if)#int g0/0/1.5

R1(config-subif)#encapsulation dot1Q 5

R1(config-subif)#description Parking

R1(config-subif)#exit

R1(config)#interface g0/0/1.6

R1(config-if)#int g0/0/1.6

R1(config-subif)#encapsulation dot1Q 6

R1(config-subif)#description Native

R1(config-subif)#exit

R1(config)#interface g0/0/1

R1(config-if)#ipv6 address fe80::1 link- local

R1(config-if)#exit

R1(config)#interface g0/0/1

```

```

R1(config-if)#no shutdown

R1#config t

R1(config)#interface loopback 0

R1(config-if)#ip address 209.165.201.1 255.255.255.224

R1(config-if)#ipv6 address 2001:db5:acad:209::1/64

R1(config-if)#ipv6 address fe80::1 link- local

R1(config-if)#no shutdown

R1(config-if)#exit

E. Comandos usados para clave cifrado rsa

R1(config)#crypto key generate rsa

general-key modulus 1024

R1(config)#

```

Tabla 4 configuración S1 y S2

Tarea	Especificaciones
Desactivar la búsqueda DNS.	No ip domain lookup
Nombre del switch	S1 o S2, según proceda Hostname S1 Hostname S2
Nombre de dominio	ccna-lab.comip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	CiscoenpassEnable secret ciscoenpass
Contraseña de acceso a la consola	CiscoconpassLine console 0Password ciscoconpassLogin
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass Username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vty 0 15Login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Transportinput ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	Banner motd "Acceso solo para personal autorizado"
Generar una clave de cifrado RSA	Módulo de 1024bits Crypto key generate rsa modulus 10242
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80:::98 para S1 y FE80:::99 para S2 Establecer la dirección IPv6 de capa 3 Int vlan 4 Ip address 10.19.8.98 255.255.255.248 Ipv6 address 2001:db5:acad:c:::98/64 Ipv6 address fe80::98 link-local Description MANAGEMENT No shutdown
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4 Ip Default-gateway 10.21.5.97

En la configuración de los switch se les asignaran nombres, se desactivara los DNS, se configurarán las VLAN, VTY, troncales y los mensajes cuando se ingresa al dispositivo de manera irregular

F. Comandos usados para configuración S1 y S2

Switch>

switch>enable

switch# config t

switch(config)# no ip domain-lookup

switch(config)# hostname S1

S1(config)#ip domain-name ccna-lab.com

S1(config)#enable secret ciscoenpass

S1(config)#line con 0

S1(config-line)#password ciscoconpass

S1(config-line)#login

S1(config-line)#exit

S1(config)#username admin privilege 15 secret admin1pass

S1(config)#line vty 0 4

S1(config-line)#login local

S1(config-line)#transport input ssh

S1(config-line)#exit

S1(config)#service password-encryption

S1(config)#banner motd "Acceso solo personal Autorizado

S1(config)#crypto key generate rsa

general-key modulus 1024

S1(config)#

G. Comandos usados para configuración S2

Switch>

switch>enable

switch# config t

switch(config)# no ip domain-lookup

switch(config)# hostname S2

S2(config)#ip domain-name ccna-lab.com

S2(config)#enable secret ciscoenpass

S2(config)#line con 0

S2(config-line)#password ciscoconpass

S2(config-line)#login

S2(config-line)#exit

S2(config)#username admin privilege 15 secret admin1pass

S2(config)#line vty 0 4

S2(config-line)#login local

S2(config-line)#transport input ssh

S2(config-line)#exit

S2(config)#service password-encryption

S2(config)#banner motd "Acceso solo personal Autorizado

S2(config)#crypto key generate rsa

general-key modulus 1024

S2(config)#

Tabla 5 configuración de S1 y S2 de la infraestructura de red (VLAN, Trunking, EtherChannel)

Tarea	Especificaciones
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, nombre Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apaga

Con la siguiente configuración en ambos switch se crearan asignándoles los nombres respectivos a la diferentes VLAN propuestas en la guía, igualmente se crearan las troncales para aumentar la capacidad de comunicación empleando el protocolo IEEE 802.1Q.

H. Comandos usados para configuración VLAN en S1 y S2

S1>enable

S1# config t

S1(config)# vlan 2

S1(config-vlan)#name Bikes

S1(config-vlan)#vlan 3

S1(config-vlan)#name Trikes

```
S1(config-vlan)#vlan 4
S1(config-vlan)#name Management
```

```
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
```

```
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native
```

```
S1(config-vlan)#exit
S1(config)#
```

I. Comandos usados para configuración Trunking en S1 con vlan 6 Nativa

```
S1>enable
```

```
S1# config t
```

```
S1(config)#interface f0/1
```

```
S1(config-if)#switchport trunk encapsulation dot1Q
```

```
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
```

```
S1(config-if)#no sh
S1(config-if)#exit
```

```
S1(config)#
```

```
S1(config)#interface f0/2
```

```
S1(config-if)#switchport trunk encapsulation dot1Q
```

```
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
```

```
S1(config-if)#no sh
S1(config-if)#exit
```

```
S1(config)#
```

```
S1(config)#interface f0/5
```

```
S1(config-if)#switchport trunk encapsulation dot1Q
```

```
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
```

```
S1(config-if)#no sh
S1(config-if)#exit
```

```
S1(config)#
```

*J. Comandos usados para configuración grupo de puertos EtherChannel
Con interfaces f0/1 y f0/2 con protocolo LACP*

```
S1>enable
```

```
S1# config t
```

```
S1(config)#interface rang f0/1-2
```

```
S1(config-if-range)#channel-protocol lacp
```

```
S1(config-if-range)#channel-group 1 mode active
```

```
S1(config-if-range)#exit
S1(config-if)#exit
```

```
S1(config)#
```

K. Comandos usados para configuración del puerto de acceso de host para VLAN 2 interface f0/6

```
S1>enable
```

```
S1# config t
```

```
S1(config)#interface f0/6
```

```
S1(config-if)#switchport mode access
```

```
S1(config-if)#switchport acces vlan 2
```

```
S1(config-if)#exit
S1(config)#
```

L. Comandos usados para configuración de seguridad del puerto en los puertos de acceso con 3 direcciones MAC

```
S1>enable
```

```
S1# config t
```

```
S1(config)#interface range f0/1-2,f0/5-6
```

```
S1(config-if-range)#switchport port-security mac-address sticky
```

```
S1(config-if-range)#switchport port-security maximum 3
```

```
S1(config-if-range)#exit
S1(config)#
```

M. Comandos usados para configuración de protección de todas las interfaces no utilizadas asignadas a VLAN 5

```
S1# config t
```

```
S1(config)#interface range f0/3-4,f0/7-24
```

```
S1(config-if-range)#switchport mode access
```

```
S1(config-if-range)#switchport access vlan 5
```

```
S1(config-if-range)#shutdown
S1(config-if-range)# switchport port-security violation shutdown
S1(config-if-range)#exit
S1(config)#
```

N. Comandos usados para configuración VLAN en S2

```
S2>enable
```

```
S2# config t
```

```
S2(config)# vlan 2
```


S2(config-vlan)#name Bikes

S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes

S2(config-vlan)#vlan 4
S2(config-vlan)#name Management

S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking

S2(config-vlan)#vlan 6
S2(config-vlan)#name Native

S2(config-vlan)#exit
S2(config)#

Ñ. Comandos usados para configuración Trunking en S2 con vlan 6 Nativa

S2>enable

S2# config t

S2(config)#interface f0/1

S2(config-if)#switchport trunk encapsulation dot1Q

S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6

S2(config-if)#no sh
S2(config-if)#exit

S2(config)#

S2(config)#interface f0/2

S2(config-if)#switchport trunk encapsulation dot1Q

S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6

S2(config-if)#no sh
S2(config-if)#exit

S2(config)#

*O. Comandos usados para configuración grupo de puertos EtherChannel
Con interfaces f0/1 y f0/2 con protocolo LACP*

S2>enable

S2# config t

S2(config)#interface rang f0/1-2

S2(config-if-range)#channel-protocol lacp

S2(config-if-range)#channel-group 1 mode active

S2(config-if-range)#exit
S2(config-if)#exit

S2(config)#

P. Comandos usados para configuración del puerto de acceso de host para VLAN 3 interface f0/18

S2>enable

S2# config t

S2(config)#interface f0/18

S2(config-if)#switchport mode access

S2(config-if)#switchport acces vlan 3

S2(config-if)#exit
S2(config)#

Q. Comandos usados para configuración de seguridad del puerto en los puertos de acceso con 3 direcciones MAC

S2>enable

S2# config t

S2(config)#interface range f0/1-2,f0/18

S2(config-if-range)#switchport port-security mac-address sticky

S2(config-if-range)#switchport port-security maximum 3

S2(config-if-range)#exit
S2(config)#

R. Comandos usados para configuración de protección de todas las interfaces no utilizadas asignadas a VLAN 5

S2# config t

S2(config)#interface range f0/3-17,f0/19-24

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 5

S2(config-if-range)#shutdown
S2(config-if-range)# switchport port-security violation shutdown
S2(config-if-range)#exit
S2(config)#

Tabla 7 configuración R1 soporte de host

Tarea	Especificaciones
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
ConfigurarIPv4DHCPpara VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las

	últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
--	---

Con esta configuración de R1 se establecen las direcciones de puerta de enlace y de los dominios.

S. Comandos usados para configuración R1 por defecto

```
R1>enable
R1#conf t
R1(config)# ip route 0.0.0.0 0.0.0.0 loopback 0
R1(config)# ipv6 route ::0 loopback 0
```

T. Comandos usados para configuración IPv4 DHCP para VLAN 2

```
R1(config)# ip dhcp excluded-address 10.21.5.1 10.21.5.52
R1(config)# ip dhcp pool vlan2-Bikes
R1(dhcp-config)# net 10.21.5.0 255.255.255.192
R1(dhcp-config)# default-router 10.21.5.1
R1(dhcp-config)# domain-name ccna-a.net
R1(dhcp-config)# exit
```

U. Comandos usados para configuración IPv4 DHCP para VLAN 3

```
R1(dhcp-config)# ip dhcp excluded-address 10.21.5.65 10.21.5.84
R1(config)# ip dhcp pool vlan3-Trikes
R1(dhcp-config)# net 10.21.5.64 255.255.255.224
R1(dhcp-config)# default-router 10.21.5.65
R1(dhcp-config)# domain-name ccna-b.net
R1(dhcp-config)# exit
R1(config)#do wr
```

Tabla 8 configuración Servidores

PC-A Network configuration	
Descripción	Comando ipconfig /all
Dirección física	000D.BDED.E316
Dirección IP	10.21.5.40
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.53
Gateway predeterminado IPv6	FE80::1
PC-B Network configuration	
Descripción	Comando ipconfig /all
Dirección física	0001.642C.6293
Dirección IP	10.21.5.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

Tabla 9 Realizando Ping

Desde	A	De Internet	IP	Resultado
PC-A	R1,G0/0/1.2	Dirección	10.21.5.1	Positivo
		IPv6	2001:db5:acad:a::1	Positivo
	R1,G0/0/1.3	Dirección	10.21.5.65	Positivo
		IPv6	2001:db5:acad:b::1	Positivo
	R1,G0/0/1.4	Dirección	10.21.5.97	Positivo
		IPv6	2001:db5:acad:c::1	Positivo
	S1,VLAN 4	Dirección	10.21.5.98	Positivo
		IPv6	2001:db5:acad:c::98	Negativo
	S2,VLAN 4	Dirección	10.21.5.99	Positivo
		IPv6	2001:db5:acad:c::99	Negativo
PC-B	PC-B	Dirección	IP address will vary	Positivo
		IPv6	2001:db5:acad:b::50	Positivo
	R1 Bucle 0	Dirección	209.165.201.1	Positivo
		IPv6	2001:db5:acad:209::1	Positivo
	R1 Bucle 0	Dirección	209.165.201.1	Positivo
		IPv6	2001:db5:acad:209::1	Positivo
	R1,G0/0/1.3	Dirección	10.21.5.65	Positivo
		IPv6	2001:db5:acad:B:1	Positivo
	R1,G0/0/1.4	Dirección	10.21.5.97	Positivo
		IPv6	2001:db5:acad:C:1	Positivo
PC-B	S1,VLAN 4	Dirección	10.21.5.98	Positivo
		IPv6	2001:db5:acad:C:98	Negativo
	S2,VLAN 4	Dirección	10.21.5.99	Positivo
		IPv6	2001:db5:acad:C:99	Negativo

Nota: En 4 de las direcciones IPv6 nos dio negativa la comunicación debido a una configuración errada en los switch y por el corto tiempo que quedaba para entregar el trabajo no logramos volver a iniciar desde cero

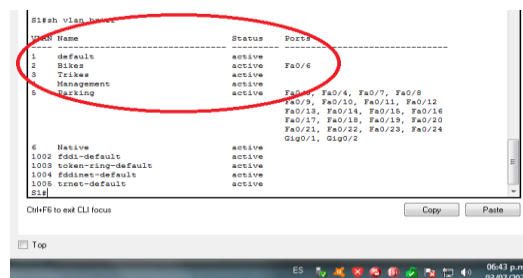


Figura 2. Show vlan brief de mi propia autoría

IV. Conclusiones

En este trabajo realizado basado en escenarios logramos mecanizar el proceso de configuración de los router y switches de una manera rápida, en el primer escenario repasamos los comandos básicos para la configuración de router y switch, como la creación de redes VLAN, asignación de direcciones IPV6, la utilización del software packettracer, asignación de contraseñas, encriptadas de las mismas, configuración DHCP, aunque se nos presentaron varias dificultades por la incompatibilidad del software y el S.O logramos realizar algunas de las actividades solicitadas, adicional para la parte final decidimos cambiar la referencia de los switch 2960 por unos multicapa de referencia 3560. Ya que con los primeros al realizar los diferentes ping de extremo a extremo el resultado fue negativo con todas las direcciones, reconfiguramos varias veces pero la falla persistía por lo tanto y sugerencia de otros compañeros realizamos el cambio obteniendo un mejor resultado aunque en las IPV6 con el PC-A ninguna dio conectividad, sin embargo la experiencia fue bastante positiva porque de la práctica de repetir los comandos aprendimos bastantes de ellos.

V. Referencias

- [1] CISCO. (s. f.). Configurar routing interVLAN en switches de capa 3. CISCO.COM. Recuperado 22 de noviembre de 2020, de <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html>
- [2] Vesga, J. Diseño y configuración de redes con packet tracer [OVA]. en línea. 2014. Noviembre de 2020. Disponible en: https://1drv.ms/u/s!AmIJYei-NT1hgCT9VCtl_pLpD9
- [3] CISCO. "Redes Conmutadas. Principios de Enrutamiento y Conmutación". {En línea}. (2019). {27 Noviembre de 2020}. Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4>
- [4] CISCO. "Redes Conmutadas. Principios de Enrutamiento y Conmutación". {En línea}. (2019). {27 Noviembre de 2020}. Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4>
- [5] CISCO. "DHCP Principios de Enrutamiento y Conmutación". [En línea]. (2019). 27 Noviembre de 2020. Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8>

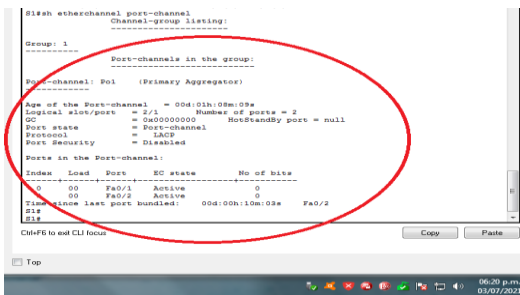


Figura 3. Show etherchannel port-channel de mi propia autoría

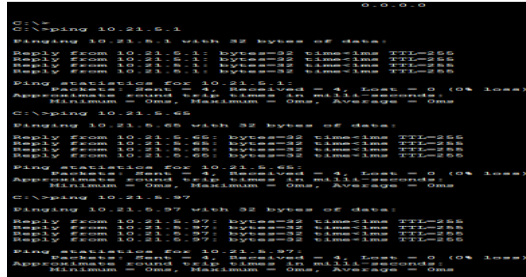


Figura 4. Haciendo ping de PC-A de mi propia autoría

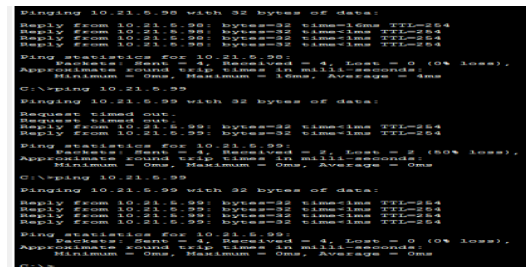


Figura 5. Haciendo ping de PC-B de mi propia autoría

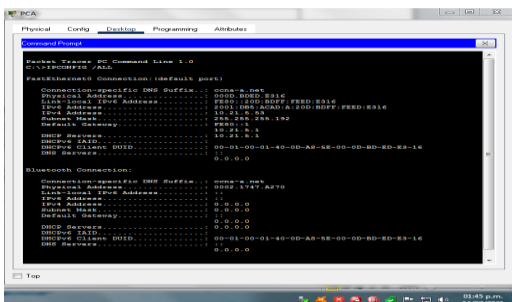


Figura 6. ipconfig /all PC-A de mi propia autoría

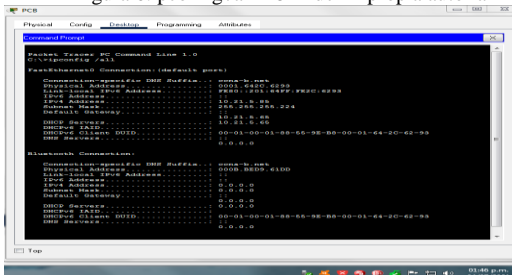


Figura 7. ipconfig /all PC-B de mi propia autoría

-
- [6] UNAD."Configuración de switches y routers[OVA]".En línea.(2017).25 Noviembre de 2020.Disponible en <https://1drv.ms/u/s!AmIJYei-NT1ihgL9QChD1m9EuGqC>

VI. Bibliografía

Sergio De J. Zapata Espinosa, Con más de 20 años de experiencia en el área de electrónica en distintas empresas a nivel regional y nacional, algún día decidí iniciar con el estudio superior en ingeniería Electrónica con el fin de concretar mucho más los conocimientos técnicos adquiridos y así poder llegar a implementar de una manera el mejoramiento o desarrollo de la solución a las situaciones que se puedan presentar en el sector.

